Chapter 3

# Number Theory

Part of G12ALN

**Contents**

# 0 Review of basic concepts and theorems

The contents of this first section – well zeroth section, really – is mostly repetition of material from last year.

Notations: $\mathbb{N} = \{1, 2, 3, \dots\}$, $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$. If $A$ is a finite set, I write $\#A$ for the number of elements in $A$.

**Theorem 0.1** (Long division)**.** *If $a, b \in \mathbb{Z}$ and $b > 0$, then there are unique integers $q$ and $r$ such that*

$$a = q\,b + r \quad \text{with} \quad 0 \leqslant r < b.$$

*Proof.* Theorem 3.2 in G11MSS. □

The integer $q$ is called the *quotient* and $r$ the *remainder*. We say that $b$ *divides* $a$ if the remainder is zero. It will be denoted by $b \mid a$.

There is an interesting variant to this: There are unique integers $q'$ and $r'$ with $a = q'\,b + r'$ and $-\frac{b}{2} < r' \leqslant \frac{b}{2}$. Instead of remainder, $r'$ is called the *least residue* of $a$ modulo $b$.

**Example.** Take $a = 62$ and $b = 9$. Then the quotient is $q = 6$ and the remainder is $r = 8$. The least residue is $r' = -1$. ◇

## 0.1 The greatest common divisor

**Definition.** Let $a$ and $b$ be integers not both equal to 0. The *greatest common divisor* of $a$ and $b$ is the largest integer dividing both $a$ and $b$. We will denote it by $(a, b)$. For convenience, we set $(0, 0) = 0$.

Let $a, b \in \mathbb{Z}$. Any sum of the form $m\,a + n\,b$, where $m$ and $n$ are integers, is called a *linear combination of $a$ and $b$.*

**Theorem 0.2.** *Let $a, b$ be integers, not both equal to 0. Then*

*i).* $(a, b) = (a, b + k\,a)$ *for all integers $k$.*

*ii).* $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.

*iii).* $(a, b)$ *is the least positive integer that is a linear combination of $a$ and $b$.*

*iv). The set of linear combinations of $a$ and $b$ is exactly the set of integer multiples of $(a, b)$.*

*Proof.* See Section 3.3 in G11MSS. □

The last part of the above shows that the ideal $a\mathbb{Z} + b\mathbb{Z}$, also denoted $(a, b)$ in ring theory, is generated by the integer $(a, b)$.

**Corollary 0.3.** *Let $a, b \in \mathbb{Z}$. An integer $d$ equals $(a, b)$ if and only if the following three conditions hold.*

- *$d \mid a$ and $d \mid b$,*
- *if $c \mid a$ and $c \mid b$ for some integer $c$, then $c \mid d$,*
- *$d > 0$.*

The definition of the greatest common divisor extends to longer lists of integers: Let $a_1, a_2, \ldots, a_n$ be integers, not all 0. Their greatest common divisor is again the largest integer dividing all of the integers in the set. It is denoted by $(a_1, a_2, \ldots, a_n)$.

**Definition.** Two integers $a, b$ are called *coprime* (or *relatively prime*) if $(a, b) = 1$. The integers $a_1, a_2, \ldots, a_n$ are called *pairwise coprime* if $(a_i, a_j) = 1$ for all $i \neq j$.

**Example.** If $a_1, a_2, \ldots, a_n$ are pairwise coprime, then $(a_1, a_2, \ldots, a_n) = 1$. The converse does not hold. For instance we have $(9, 8, 6) = 1$, however they are not pairwise coprime as $(9, 6) = 3$. ◇

**Aside:** How likely is it that two "random" integers are coprime? More precisely, the probability that two random integer smaller than $N$ are coprime is a function in $N$. How does it behave as $N \to \infty$? Answer it converges to $\frac{6}{\pi^2}$. When $N$ is large about 60.79% of pairs of integers are coprime. ◇

**Lemma 0.4** (Euclid's Lemma)**.** *If $a, b, c$ are integers such that $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.*

*Proof.* Corollary 3.15 in G11MSS. □

**Corollary 0.5.** *If $a$, $b$ and $n > 1$ are integers such that $a \mid n$ and $b \mid n$ and $(a, b) = 1$, then $ab \mid n$.*

*Proof.* Since $a$ divides $n$, there is an integer $k$ such that $n = a\,k$. Now $b$ divides $a\,k$. By Lemma 0.4, $b$ divides $k$ since $a$ and $b$ are coprime. Therefore $k = b\,k'$ for some integer $k'$. Hence $n = abk'$ proves the corollary. □

**Theorem 0.6** (Euclidean Algorithm)**.** *Let $a, b \in \mathbb{Z}$ be such that $a \geqslant b > 0$. Set $r_0 = a$ and $r_1 = b$. For $i > 1$, define recursively $r_i$ to be the remainder when dividing $r_{i-2}$ by $r_{i-1}$. Then the last non-zero entry in the sequence $r_0, r_1, \ldots$ is equal to the greatest common divisor of $a$ and $b$.*

In detail, we have a chain of equations:

$$\begin{aligned} r_0 &= q_1\, r_1 + r_2 \\ r_1 &= q_2\, r_2 + r_3 \\ &\vdots \quad\quad \vdots \\ r_{n-2} &= q_{n-1}\, r_{n-1} + r_n \\ r_{n-1} &= q_n\, r_n. \end{aligned}$$

Say $r_{n+1} = 0$ and $r_n \neq 0$, then $(a, b) = r_n$.

*Proof.* Section 3.3 in G11MSS. □

**Example.** We compute that the greatest common divisor of 9633 and 3016 is 13.

$$\begin{aligned} 9633 &= 3 \cdot 3016 + 585 \\ 3016 &= 5 \cdot 585 + 91 \\ 585 &= 6 \cdot 91 + 39 \\ 91 &= 2 \cdot 39 + 13 \\ 39 &= 3 \cdot 13 \end{aligned}$$

"Working backwards" we can express $(9633, 3016) = 13$ as a linear combination of 9633 and 3016:

$$\begin{aligned} 13 &= 91 - 2 \cdot 39 \\ &= 91 - 2 \cdot (585 - 6 \cdot 91) = 13 \cdot 91 - 2 \cdot 585 \\ &= 13 \cdot (3016 - 5 \cdot 585) - 2 \cdot 585 = 13 \cdot 3016 - 67 \cdot 585 \\ &= 13 \cdot 3016 - 67 \cdot (9633 - 3 \cdot 3016) = -67 \cdot 9633 + 214 \cdot 3016 \end{aligned}$$

◇

**Aside:** *Implementation of the euclidean algorithm.* Here is the pseudo-code how this algorithm is implemented. In these lecture notes, pseudo-code is written using the syntax of `python` with minor modifications. For instance in python one should write % instead of "`mod`" in the following code.

```
def gcd(a,b):
    while b > 0:
        (a, b) = (b, a mod b)
    return a
```

The extended version gives also one possible pair $x$ and $y$ such that $(a, b) = x\,a + y\,b$.

```
def extended_gcd(a, b):
    (x, y, u, v) = (1, 0, 0, 1)
    while b > 0:
        q = a//b
        (a, b) = (b, a mod b)
        (x, y, u, v) = (u, v, x - u*q, y - v*q)
    return a, x, y
```

Here `a//b` returns the quotient of `a` divided by `b` without remainder; e.g. `7//3` returns 2. ◇

**Example.** Here an example why mathematical proofs are important. Is it true that $n^5 - 5$ is coprime to $(n+1)^5 - 5$ for all $n > 0$ ? Certainly it looks like to be true as it holds for all $n < 10^6$. However it is not true. For $n = 1435390$ the greatest common divisor of $n^5 - 5 = 609325819747632930116416989999 5$ and $(n+1)^5 - 5 = 609327942260220979624459183794 6$ is equal to the prime number 1968751. If you know what a resultant is, there is a simple reason for this. ◇

## 0.2 Primes

**Definition.** A natural number $p$ is called a *prime* if $p > 1$ and the only positive divisors of $p$ are 1 and $p$ itself. A number $n > 1$ that is not a prime is called *composite*.

**Theorem 0.7.** *There are infinitely many primes.*

*Proof.* Section 2.7 in G11ACF. □

**Aside:** *Further results on primes.* Dirichlet proved the following result. Let $a$ and $m > 1$ be coprime integers. Then there are infinitely many primes in the arithmetic progression $a$, $a+m$, $a+2m$, ... For this and more, go to G13FNT next year!

Primes become sparser and sparser. In some vague sense, the likelihood that a large integer $n$ is prime is approximately $1/\log(n)$. Here is how many primes there are below $N$ for some values of $N$:

| $N$ | $10^3$ | $10^4$ | $10^5$ | $10^6$ | $10^7$ | $10^8$ | $10^9$ |
|---|---|---|---|---|---|---|---|
| # primes | 168 | 1229 | 9592 | 78498 | 664579 | 5761455 | 50847534 |

However there are many open problems about prime numbers. Here a list of three of them:

- Goldbach's Conjecture: Every even positive integer greater than 2 can be written as a sum of two primes.
- Twin prime conjecture: There are infinitely many pairs of primes $p$ and $q$ with $q = p + 2$.
- Landau's conjecture: There are infinitely many primes of the form $n^2+1$ with $n \in \mathbb{Z}$.

Recently (2013), it was shown by Helfgott that every odd integer greater than 5 can be written as a sum of three primes. Based on initial work by Yitang Zhang in 2013, we know now that there are infinitely many prime pairs $p > q$ with $p - q < 246$. ◇

**Theorem 0.8** (The fundamental theorem of arithmetic)**.** *Every positive integer $n > 1$ can be written as a product of primes. The product is unique up to reordering the factors.*

*Proof.* Theorem 3.19 in G11MSS. □

Explicitly, every integer $n > 1$ can be written as

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$$

for some integer $r \geqslant 1$, some *distinct* prime numbers $p_1$, $p_2$, …, $p_r$ and some integers $a_1 \geqslant 1$, $a_2 \geqslant 1$, …, $a_r \geqslant 1$. Up to permuting the primes, this is unique. For instance $13! = 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$.

**Corollary 0.9.** *Suppose that $a, b$ are two positive integers with prime factorisations: $a = \prod_{i=1}^{r} p_i^{a_i}$ and $b = \prod_{j=1}^{s} q_j^{b_j}$ where $p_i$ and $q_j$ are primes. Then the prime factorisation of $(a, b)$ is $\prod_k p_k^{c_k}$ with the product running only over all $1 \leqslant k \leqslant r$ for which there is a $1 \leqslant j \leqslant s$ with $q_j = p_k$ and where $c_k = \min\{a_k, b_j\}$.*

**Example.** The greatest common divisor of 1000 and 1024 is 8, because $1000 = 2^3 \cdot 5^3$ and $1024 = 2^{10}$. ◇

## 0.3 Congruences

**Definition.** Let $m \geqslant 1$ be a positive integer. If $a, b$ are integers, we say that $a$ is *congruent to $b$ modulo $m$* if $m$ divides $a - b$. We write $a \equiv b \pmod{m}$. The integer $m$ is called the *modulus* of the congruence.

Given an integer $a$. The set of all integers $b$ such that $a \equiv b \pmod{m}$ is called a *congruence class modulo $m$* and is denoted by $[a]$ or $a + m\mathbb{Z}$.

The set of all congruence classes modulo $m$ is denoted by $\mathbb{Z}/m\mathbb{Z}$.

You will see people using the notation "$a \bmod m = b$". We will refrain from using this, which is often meant to mean that $b$ is the remainder of $a$ modulo $m$. Note that $\equiv$ will always mean congruences and never vague things like "identically equal to".

The set $\mathbb{Z}/m\mathbb{Z}$ comes with a natural ring structure: If $a, b \in \mathbb{Z}$. We set $[a] + [b] = [a + b]$ and $[a] \cdot [b] = [ab]$. This comes as no surprise when thinking of quotients of rings by ideals; otherwise just check that the definition of these operations do not depend on the choice of $a$ and $b$ in the coset: For instance if $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, then there exists $k \in \mathbb{Z}$ and $l \in \mathbb{Z}$ with $a = a' + km$ and $b = b' + lm$ and hence $a \cdot b = a' \cdot b' + (kb' + la' + kl)m \equiv a'b' \pmod{m}$.

**Example.** $\mathbb{Z}/10\mathbb{Z}$ is the set $\{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9]\}$. We can write $1234 \equiv 44 \equiv -6 \pmod{10}$ or equivalently $[1234] = [44] = [-6]$ and they are equal to $[4]$. The operations look like $[13]+[19] = [13+19] = [32]$; of course this is the same as $[3]+[9] = [2]$. In other words, operations on $\mathbb{Z}/10\mathbb{Z}$ are just manipulations regarding only the last digit of positive integers.

Similarly the clock (neglecting am and pm) is an example of working modulo 12: "Three hours after 11 o'clock, it is 2 o'clock" reads $[3]+[11] = [2]$ in $\mathbb{Z}/12\mathbb{Z}$ or $3 + 11 \equiv 2 \pmod{12}$. ◇

Recall that the unit group $R^*$ of a ring is the set of its invertible elements, i.e., all $a \in R$ such that there is $b \in R$ with $ab = 1_R$.

**Proposition 0.10.** *The unit group $(\mathbb{Z}/m\mathbb{Z})^*$ consists of all congruence classes $[a]$ with $a$ coprime to $m$.*

*Proof.* If $[a]$ is invertible in the ring $\mathbb{Z}/m\mathbb{Z}$, then there is a congruence class $[b]$ with $[b]\cdot[a] = [1]$. This equation is equivalent to $ba \equiv 1 \pmod{m}$ and to $ba = 1 + km$ for some integer $k$. If $d$ divides both $a$ and $m$, then $d$ also divides $1 = km - ab$. Hence $d = 1$. Therefore $a$ and $m$ are coprime.

Conversely, if $a$ is coprime to $m$, then there are integers $b$ and $k$ such that $ba + km = (a, b) = 1$. Hence $b \cdot a \equiv 1 \pmod{m}$ shows that $[a]$ is invertible. □

If $m = p$ is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field, often denoted by $\mathbb{F}_p$. For all composite $m$, the ring $\mathbb{Z}/m\mathbb{Z}$ has zero-divisors and it is therefore not a field.

Recall that we can use the euclidean algorithm as in Theorem 0.6 to find an inverse $b$ of $a$ modulo $m$: By working backwards after computing that $(a, m) = 1$, we find integers $b$ and $k$ such that $b\,a + k\,m = 1$. Therefore $b\,a \equiv 1 \pmod{m}$.

**Example.** The inverse of 99 modulo 1307 is computed as follows:

$$\begin{aligned} 1307 &= 13 \cdot 99 + 20 \\ 99 &= 4 \cdot 20 + 19 \\ 20 &= 1 \cdot 19 + 1 \end{aligned}$$

Then working backwards

$$\begin{aligned} 1 &= 20 - 1 \cdot 19 = 20 - 1 \cdot (99 - 4 \cdot 20) = 5 \cdot 20 - 1 \cdot 99 \\ &= 5 \cdot (1307 - 13 \cdot 99) - 1 \cdot 99 \equiv (-66) \cdot 99 \pmod{1307} \end{aligned}$$

Hence the inverse of $[99]$ is $[-66]$. ◇

# 1 Congruence equations

In this section, we will ask ourselves how to solve equations modulo $m$. For instance find all solutions to $x^7+xy+13 \equiv 0 \pmod{1000}$ in $x$ and $y$. First, we will answer this completely for linear equations in one variable. Then we will show ow one can reduce the question to moduli which are prime powers and then how to reduce it to the case when the modulus is a prime.

## 1.1 Linear congruence equation

We will try to solve the following linear congruence equation in one variable:

$$a\,x \equiv b \pmod{m} \tag{1}$$

where $a$, $b$ and $m > 1$ are given integers.

**Proposition 1.1.** *Suppose $a$ and $m$ are coprime. Then the solutions to equation (1) form exactly one congruence class modulo $m$.*

*Proof.* If $(a, m) = 1$, then $[a]$ is a unit in $\mathbb{Z}/m\mathbb{Z}$ by Proposition 0.10. So there is an inverse class $[a^*]$ with $[a][a^*] = 1$. The equation (1) is equivalent to $[a][x] = [b]$, which is equivalent to $[x] = [a^*][b]$. □

**Theorem 1.2.** *Let $d = (a, m)$. If $d \nmid b$, then (1) has no solutions. If $d \mid b$, then (1) has exactly $d$ incongruent solutions modulo $m$.*

*Proof.* The equation (1) has a solution if there is an integer $k$ such that $ax = b + km$. If $d \nmid b$, then there are no solutions.

Now suppose that $b = d \cdot b'$. Write $m = d \cdot m'$ and $a = d \cdot a'$. We may divide the above equation by $d$ to get $a'x = b' + km'$. Hence the solutions to (1) are the same as to the equation

$$a'\,x \equiv b' \pmod{m'}.$$

By the first part of Theorem 0.2, we know that $a'$ and $m'$ are coprime. Therefore we may apply the previous proposition. There is an integer $x_0$ such that the solutions to our equation are all integers of the form $x = x_0 + n\,m'$ for some integer $n$. The congruence class modulo $m'$

splits up into $d$ congruence classes modulo $m$: The solutions $x_0$, $x_0 + m'$, $x_0 + 2\,m'$, $\ldots$, $x_0 + (d-1)\,m'$ are incongruent modulo $m$. □

**Example.** As $(33, 21) = 3$, we should expect 3 residue classes to satisfy $21x \equiv 15 \pmod{33}$. Indeed, the congruence is equivalent to $7x \equiv 5 \pmod{11}$. Now 7 is the inverse of 8 modulo 11. Hence we get $x \equiv 8{\cdot}5 \equiv 7 \pmod{11}$. Hence the solutions are [7], [18] and [29] modulo 33. ◇

## 1.2 The Chinese remainder theorem

**Lemma 1.3.** *Let $m$ and $n$ be coprime positive integers. Let $a$ and $b$ be two integers. Then the solutions to the system of congruences*

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

*is a unique congruence class modulo $m \cdot n$.*

*Proof.* Existence: Since $m$ and $n$ are coprime, there are integers $A$ and $B$ such that $Am + Bn = 1$. Set $x = b\,Am + a\,Bn$. Since $Bn \equiv 1 \pmod{m}$, we obtain $x \equiv a \pmod{m}$. Similarly $x \equiv b \pmod{n}$.

Uniqueness: If $x$ and $y$ are two solutions, then $m$ and $n$ both divide $x - y$ as $x \equiv y \pmod{m}$ and $x \equiv y \pmod{n}$. Since $m$ and $n$ are coprime, Corollary 0.5 implies that $mn$ divides $x - y$. Therefore $x \equiv y \pmod{nm}$. □

Note that this also follows from the more general "Chinese remainder theorem", Theorem 2.3.7, in G12ALN. One takes $I = m\mathbb{Z}$ and $J = n\mathbb{Z}$. Then $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Take $[x]$ to be the unique element in the left hand-side that corresponds to $\big([a], [b]\big)$ on the right hand-side.

**Theorem 1.4** (Chinese remainder theorem)**.** *Let $m_1, m_2, \ldots, m_r$ be pairwise coprime positive integers. Then the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

*has a unique solution modulo $m_1 \cdot m_2 \cdots m_r$.*

*Proof.* By induction on $r$. There is nothing to do for $r = 1$. Write $n = m_1 \cdot m_2 \cdots m_{r-1}$ and $m = m_r$. By induction, there is a unique $a$ modulo $n$ that satisfies the first $r-1$ equations. Now apply the Lemma 1.3 with $b = a_r$. □

**Example.** The age of the captain is an odd number that when divided by 5 has remainder 3 and when divided by 11 has remainder 8. How old is the captain?

For $x \equiv 3 \pmod 5$ and $x \equiv 8 \pmod{11}$. Since $1 \cdot 11 + (-2) \cdot 5 = 1$, we see that these two combine to $x \equiv 3 \cdot 1 \cdot 11 + 8 \cdot (-2) \cdot 5 = -47 \equiv 8 \pmod{55}$. Then $x \equiv 8 \pmod{55}$ and $x \equiv 1 \pmod 2$ combine to $x \equiv 63 \pmod{110}$. ◇

## 1.3 Non-linear equations

We now turn to more general equations. Let $m > 1$ be an integer. Let $f(x, y, z, \dots)$ be a polynomial in (finitely many) variables and integer coefficients. In the linear case, we had $f(x) = ax - b$. We wish to find all solutions to

$$f(x, y, z, \dots) \equiv 0 \pmod m. \tag{2}$$

Given a polynomial $f$ as above, we will write $\mathrm{NSol}_f(m)$ for the number of solutions modulo $m$; more precisely this is the number of vectors $([x], [y], [z], \dots)$ with entries in $\mathbb{Z}/m\mathbb{Z}$ such that $f(x, y, z, \dots) \equiv 0 \pmod m$. (More generally, we could ask for systems of such polynomial congruence equations.)

**Example.** Consider $f(x, y) = y^2 - x^3 - x - 1$. Here are the first few values of $\mathrm{NSol}_f(m)$.

| $m$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mathrm{NSol}_f(m)$ | 2 | 3 | 2 | 8 | 6 | 4 | 4 | 9 | 16 | 13 | 6 | 17 | 8 |
| $m$ | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| $\mathrm{NSol}_f(m)$ | 24 | 8 | 17 | 18 | 20 | 16 | 12 | 26 | 27 | 12 | 40 | 34 | 27 |

For instance the solutions to $f(x, y) \equiv 0 \pmod 7$ are $([0], [1])$, $([0], [-1])$, $([2], [2])$, and $([2], [-2])$. ◇

**Proposition 1.5.** *Let $f$ be a polynomial with integer coefficient.*

- *If $n$ and $m$ are two coprime integers, then*

$$\mathrm{NSol}_f(n \cdot m) = \mathrm{NSol}_f(n) \cdot \mathrm{NSol}_f(m).$$

- *Let $m = \prod_{i=1}^{r} p_i^{a_i}$ be the prime factorisation of an integer $m$. Then*

$$\mathrm{NSol}_f(m) = \prod_{i=1}^{r} \mathrm{NSol}_f(p_i^{a_i}).$$

*Proof.* We use Lemma 1.3. First, if $(x+mn\mathbb{Z}, y+mn\mathbb{Z}, \dots)$ is a solution modulo $nm$, then $(x + m\mathbb{Z}, y + m\mathbb{Z}, \dots)$ is a solution modulo $m$ and $(x+n\mathbb{Z}, y+n\mathbb{Z}, \dots)$ is a solution modulo $n$. Conversely, if $(a+m\mathbb{Z}, a'+m\mathbb{Z}, \dots)$ is a solution modulo $m$ and $(b+n\mathbb{Z}, b'+n\mathbb{Z}, \dots)$ is a solution modulo $n$, then Lemma 1.3 guarantees us a that there is a $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$, and a $y \equiv a' \pmod{m}$ and $y \equiv b' \pmod{n}$, etc. In other words $(x + nm\mathbb{Z}, y + nm\mathbb{Z}, \dots)$ is a solution modulo $nm$. Hence solutions modulo $nm$ are in bijection with pairs of solutions modulo $m$ and $n$.

The second part is deduced from the first by induction on the number of prime factors of $m$. □

The example above shows that that $\mathrm{NSol}_f(nm)$ and $\mathrm{NSol}_f(n)\cdot\mathrm{NSol}_f(m)$ can differ when $(n, m) \neq 1$.

**Example.** Consider the polynomial $f(x) = x^2 + 1$. It has two solutions modulo 5, namely [2] and [3]. It also has two solutions modulo 13, namely [5] and [8]. Therefore, the above proposition implies that $f(x) \equiv 0 \pmod{65}$ has four solutions. Indeed they are [8], [18], [47] and [57].

Note in particular that this is an example of a polynomial with more solutions than its degree. If $g(x) \in k[x]$ with $k$ a field, there are always at most $\deg(g)$ solutions. However $\mathbb{Z}/65\mathbb{Z}$ is not a field. ◇

The proposition tells us that we may restrict now to the case when $m$ is a prime power when trying to solve (2).

## 1.4 Lifting solutions

Let $p$ be a prime. The aim of this section is to explain how one can (sometimes) get from a solution modulo $p$ to a solution modulo powers of $p$. This process is called "lifting" a solution. We illustrate this first with an example.

**Example.** Consider the equation $f(x) = x^2 + 1 \equiv 0 \pmod 5$. Checking all congruence classes modulo $p = 5$, we find that $x_0 = 2$ and $x_1 = 3$ are the only two solutions.

Now we consider $x^2 + 1 \equiv 0 \pmod{25}$. If $x$ is a solution modulo 25 then its remainder modulo 5 is a solution modulo 5. So we can write $x$ as $2 + t \cdot 5$ or $3 + t \cdot 5$ for some integer $t$. We plug this into the equation to get

$$\begin{aligned} & 0 \equiv (2 + t \cdot 5)^2 + 1 = 5 + 4t \cdot 5 + t^2 \cdot 5^2 \pmod{25} \\ \iff \quad & 0 \equiv 5 + 4t \cdot 5 \pmod{25} \\ \iff \quad & 0 \equiv 1 + 4t \pmod 5 \\ \iff \quad & t \equiv 1 \pmod 5 \end{aligned}$$

where we used how to solve the resulting linear equation. So we find that $2 + 1 \cdot 5 = 7$ is a solution modulo 25. The only other solution is $3 + 3 \cdot 5 = 18$. ◇

**Definition.** If $f(x) = a_0 + a_1\, x + a_2\, x^2 + \cdots + a_d x^d$ is a polynomial with coefficients in $\mathbb{Z}$, we define its *derivative* by $f'(x) = a_1 + 2\, a_2\, x + 3\, a_3\, x^2 + \cdots + d\, a_d\, x^{d-1}$. It is again a polynomial with coefficients in $\mathbb{Z}$.

**Lemma 1.6.** *Let $f(x) \in \mathbb{Z}[x]$ and set $g(x) = f(x + a)$ for some integer $a$. Then $g'(x) = f'(x + a)$.*

*Proof.* If we relate this back to the usual definition of the derivative of real functions, then the lemma follows immediately from the chain rule. If we want to avoid limits, then we can do the following. Write $f(x) = \sum_{k=0}^{d} c_k x^k$. Then $g(x) = \sum_{k=0}^{d} c_k \sum_{i=0}^{k} \binom{k}{i} a^{k-i} x^i$ and we can

compute

$$\begin{aligned} g'(x) &= \sum_{k=0}^{d} c_k \sum_{i=1}^{k} i \binom{k}{i} a^{k-i} x^{i-1} \\ &= \sum_{k=0}^{d} c_k \sum_{j=0}^{k-1} (j+1) \binom{k}{j+1} a^{k-(j+1)} x^{j} \\ &= \sum_{k=0}^{d} c_k \sum_{j=0}^{k-1} k \binom{k-1}{j} a^{(k-1)-j} x^{j} \\ &= \sum_{k=0}^{d} c_k \, k \, (x+a)^{k-1} = f'(x+a). \end{aligned}$$ □

**Theorem 1.7** (Hensel's Lemma)**.** *Let $p$ be a prime and $k \geqslant 1$. Let $f(x)$ be a polynomial with coefficients in $\mathbb{Z}$. Suppose $x_0$ is a solution of $f(x) \equiv 0 \pmod{p^k}$ such that $f'(x_0) \not\equiv 0 \pmod{p}$. Then there is a unique $t$ modulo $p^k$ such that $x_0 + t\,p^k$ is a solution to $f(x) \equiv 0 \pmod{p^{2k}}$.*

*Proof.* Write $\xi = x - x_0$. Plug $x = \xi + x_0$ into $f$ and expand it as a polynomial in the new unknown $\xi$. We get $f(\xi + x_0) = a_0 + a_1\,\xi + a_2\,\xi^2 + \cdots + a_d\,\xi^d$ for some integers $a_i$. We note that $a_0 = f(x_0)$ is divisible by $p^k$, say $a_0 = p^k\,b$. By the previous lemma, we find that $a_1 = f'(x_0)$, which is not divisible by $p$. Now we wish to find the solutions to $f(x) \equiv 0 \pmod{p^{2k}}$ with $\xi = t\,p^k$:

$$\begin{aligned} & 0 \equiv a_0 + a_1\,t\,p^k + a_2\,t^2\,p^{2k} + \cdots + a_d\,t^d\,p^{dk} \pmod{p^{2k}} \\ \iff \quad & 0 \equiv a_0 + a_1\,t\,p^k \pmod{p^{2k}} \\ \iff \quad & 0 \equiv p^k \cdot (b + a_1\,t) \pmod{p^{2k}} \\ \iff \quad & 0 \equiv b + a_1\,t \pmod{p^k} \end{aligned}$$

We are reduced to solve a linear congruence. Since $p$ does not divide $a_1$, the latter is coprime to $p^k$. Therefore there is a unique solution for $t$ modulo $p^k$ by Proposition 1.1. □

**Example.** We know that 18 is a solution to $x^2 + 1 \equiv 0$ modulo 25. We have $f'(18) = 2 \cdot 18 \not\equiv 0 \pmod{5}$. So the theorem applies to give us a solution modulo $5^4$.

Explicitly, we need to solve $0 \equiv b + a_1\,t$ modulo 25 with $a_1 = f'(18) \equiv 11 \pmod{25}$ and $b = f(18)/25 = 13$. Now solve the equation $0 \equiv 13 + 11\,t \pmod{25}$: the inverse of 11 modulo 25 is 16, hence $t \equiv -13 \cdot 11 \equiv 17 \pmod{25}$. This gives $x = 18 + 17 \cdot 25 = 443$ is a solution to $x^2 + 1 \equiv 0$ modulo $5^4$. ◇

It is also clear from the proof above that we have two further cases. If $f'(x_0) \equiv 0 \pmod{p}$ and $f(x_0) \not\equiv 0 \pmod{p^{2k}}$, then there is no solution for $t$. If $f'(x_0) \equiv 0 \pmod{p}$ and $f(x_0) \equiv 0 \pmod{p^{2k}}$ then all $t$ are solutions.

**Corollary 1.8.** *If there exists a solution $x_0$ to $f(x) \equiv 0 \pmod{p}$ with $f'(x_0) \not\equiv 0 \pmod{p}$. Then there exists a solution to $f(x) \equiv 0 \pmod{p^k}$ for all $k > 1$, too.*

**Example.** When the condition $f'(x_0) \not\equiv 0 \pmod{p}$ is not satisfied, it is more complicated. The polynomial $f(x) = x^2 + x + 7$ has a solutions $x_0 = 1$ modulo 9, yet no solutions modulo 27 or any higher power of 3. This is because $f'(1) \equiv 0 \pmod{3}$, but $f(1) \not\equiv 0 \pmod{27}$. Now $x^2 + x + 25$ will have a solution $x_0 = 1$ modulo 27, but none modulo 81.

For instance the polynomial $x^3 - 3\,x + 2$ has a solution $x_0 = 1$ modulo all powers of 3, yet Hensel's Lemma never applies. ◇

**Aside:** *T*his is the starting point to the construction of "$p$-adic numbers". They form an interesting field containing $\mathbb{Q}$ incorporating working with polynomial equations modulo $p^k$ for all $k$ at once. They really should stand on equal footing with the real numbers as they can be obtained by the same completion process. But that is very exciting material for G13FNT and G14ANT. ◇

A concluding remark on this section. Given a polynomial equation, we have seen how to use the Chinese remainder theorem to reduce the question to $m = p^k$ for a prime number $k$. Then Hensel's lemma allows us often to answer it for a prime powers by solving it for $m = p$. This leaves the question of how to solve polynomial equations modulo primes $p$. For small primes $p$, one can just run through all values, but for large $p$ this is far from being efficient. There is a lot of on-going research in this direction.

# 2 Arithmetic functions

In this section, we will study functions like the Euler totient function that measure arithmetic properties of numbers. Typical questions could be: How many prime factors does a very large number have in average?

**Definition.** A function $f\colon \mathbb{N} \to \mathbb{C}$ is called an *arithmetic function*. Such a function $f$ is called *multiplicative* if $f(mn) = f(m)f(n)$ for all pairs of coprime positive integers $m, n$. It is called *completely multiplicative* if $f(mn) = f(m)f(n)$ for all positive integers $m$ and $n$.

**Example.** The function $f(n) = n^s$ is completely multiplicative for any real number $s$. Given a polynomial $f(x, y, z, \dots)$ with integer coefficients, by Proposition 1.5 the function $\mathrm{NSol}_f$ is multiplicative, but not completely multiplicative in general. ◇

## 2.1 The Euler phi-function

**Definition.** Let $n$ be a positive integer. *Euler's phi-function* $\varphi(n)$ is defined to be the number of units in $\mathbb{Z}/n\mathbb{Z}$. It is also called *Euler's totient function*. By Proposition 0.10, we obtain

$$\varphi(n) = \#\Big\{a \;\Big|\; 1 \leqslant a < n \text{ and } (a, n) = 1\Big\}$$

Here is a table with some values of Euler's $\varphi$-function.

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\varphi(n)$ | 1 | 1 | 2 | 2 | 4 | 2 | 6 | 4 | 6 | 4 | 10 | 4 | 12 | 6 |
| $n$ | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| $\varphi(n)$ | 8 | 8 | 16 | 6 | 18 | 8 | 12 | 10 | 22 | 8 | 20 | 12 | 18 | 12 |

In Figure 1, there is a plot of the values up to 1000.

**Theorem 2.1.** *Euler's phi function is multiplicative, but not completely multiplicative.*

*Proof.* Let $m$ and $n$ be coprime natural numbers. We show that the map

$$\Psi\colon \big(\mathbb{Z}/mn\mathbb{Z}\big)^* \to \big(\mathbb{Z}/m\mathbb{Z}\big)^* \times \big(\mathbb{Z}/n\mathbb{Z}\big)^*$$
$$x + nm\mathbb{Z} \mapsto \big(x + m\mathbb{Z}, x + n\mathbb{Z}\big)$$

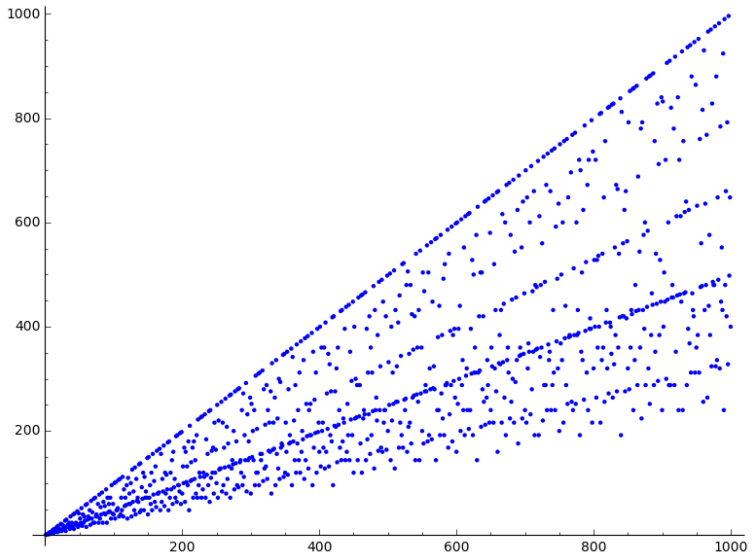



Figure 1: First 1000 values of $\varphi$

is a bijection. First note that the map is well defined in that, if we replace $x$ by $x' = x + knm$ for some $k \in \mathbb{Z}$, then $x + m\mathbb{Z} = x' + m\mathbb{Z}$ and $x + n\mathbb{Z} = x' + n\mathbb{Z}$. Also $x + nm\mathbb{Z}$ is invertible if and only if $(x, nm) = 1$. Using Euclid's Lemma 0.4, this is equivalent to $(x, n) = 1$ and $(x, m) = 1$ because $(n, m) = 1$. Hence $\Psi$ sends invertible elements to pairs of invertible elements.

Now if $\Psi(x + nm\mathbb{Z}) = \Psi(x' + nm\mathbb{Z})$, then $x \equiv x' \pmod{n}$ and $x \equiv x' \pmod{m}$. Now the Chinese remainder Theorem as in Lemma 1.3 shows that $x \equiv x' \pmod{nm}$. Therefore $\Psi$ is injective. The same lemma also shows that $\Psi$ is surjective: Take $(a + m\mathbb{Z}, b + n\mathbb{Z})$ in the target of $\Psi$. Then there exists $x$ such that $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$. Then $\Psi(x + nm\mathbb{Z}) = (a + m\mathbb{Z}, b + n\mathbb{Z})$. We have shown that $\Psi$ is a bijection.

Therefore $\varphi(m\,n) = \#(\mathbb{Z}/mn\mathbb{Z})^* = \#(\mathbb{Z}/m\mathbb{Z})^* \cdot \#(\mathbb{Z}/n\mathbb{Z})^* = \varphi(m) \cdot \varphi(n)$ shows that $\varphi$ is multiplicative. Since $\varphi(4) \neq \varphi(2) \cdot \varphi(2)$, it is not completely multiplicative. □

Note that Corollary 2.3.8 in G12ALN with $R = \mathbb{Z}$, $I_1 = m\mathbb{Z}$ and $I_2 = n\mathbb{Z}$ yields that

$$(\mathbb{Z}/mn\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*.$$

is not just a bijection but a group isomorphism.

**Proposition 2.2.** *If $n = \prod_{i=1}^{r} p_i^{a_i}$ is the prime factorisation of $n$, then*

$$\varphi(n) = \prod_{i=1}^{r} \left( p_i^{a_i} - p_i^{a_i - 1} \right) = n \cdot \prod_{p \mid n} \left( 1 - \frac{1}{p} \right)$$

*where the last product runs over all prime divisors $p$ of $n$.*

*Proof.* This is the content of Corollary 2.5.5 in G12ALN. First the previous theorem implies that $\varphi(n) = \prod_i \varphi\left(p_i^{a_i}\right)$. Let $k \geqslant 1$. Now to be coprime to $p^k$ is the same as to be coprime to $p$. So from all $p^k$ values in the range $1 \leqslant a \leqslant p^k$, we will not allow $p^{k-1}$ one of them, namely $p$, $2p$, $\ldots$, $p^k$. This gives $\varphi(p^k) = p^k - p^{k-1}$. □

**Aside:** *More on $\varphi(n)$.* The average of all values $\varphi(k)$ for $1 \leqslant k \leqslant n$ stays close to $\frac{3}{\pi^2} n$. One has this remarkable limit statement

$$\liminf \frac{\varphi(n) \cdot \log(\log(n))}{n} = e^{-\gamma} \approx 0.5614\ldots$$

where $\gamma$ is the Euler-Mascheroni constant. However there are infinitely many $n$ for which the fraction on the left is smaller than $e^{-\gamma}$.

Using the formula in Proposition 2.2 it is possible to compute $\varphi(n)$ if the factorisation of $n$ is known. Conversely, if we know how to compute it fast without factoring, we could break the RSA cryptosystem. ◇

## 2.2 Divisor functions

**Definition.** The *sum of divisors function* $\sigma$ is defined by setting $\sigma(n)$ equal to the sum of all positive divisors of $n$. The *number of divisors function* $\tau$ is defined by setting $\tau(n)$ equal to the number of positive divisors of $n$.

We may write $\sigma(m) = \sum_{d \mid m} d$ and $\tau(m) = \sum_{d \mid m} 1$. The notation $\sum_{d \mid n}$ will always stand for the sum over $d$ running through all positive divisors of $n$. For instance, for a prime $p$, we have $\tau(p) = 2$ and $\sigma(p) = p + 1$.

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\sigma(n)$ | 1 | 3 | 4 | 7 | 6 | 12 | 8 | 15 | 13 | 18 | 12 | 28 | 14 | 24 | 24 |
| $\tau(n)$ | 1 | 2 | 2 | 3 | 2 | 4 | 2 | 4 | 3 | 4 | 2 | 6 | 2 | 4 | 4 |

The first thousand values of $\sigma$ and $\tau$ are plotted in Figure 2.

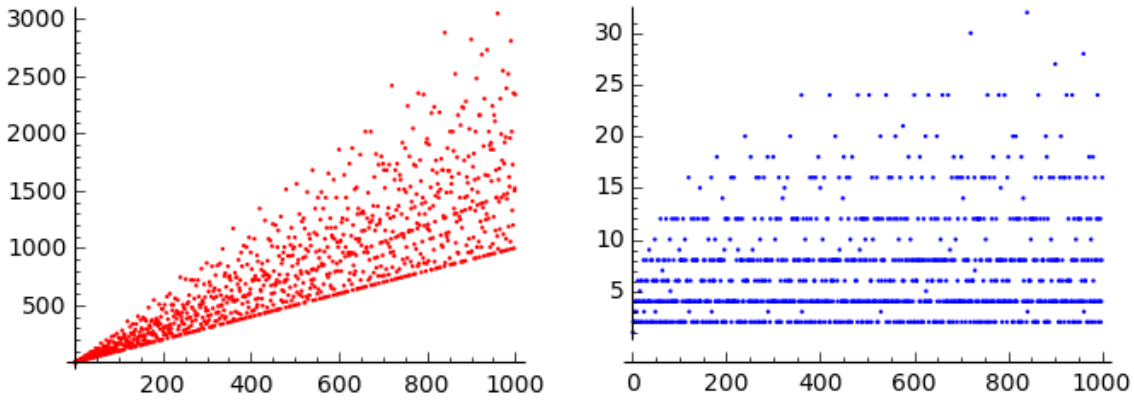



Figure 2: Values of $\sigma(n)$ on the left and of $\tau(n)$ on the right

**Theorem 2.3.** *The arithmetic functions $\sigma$ and $\tau$ are multiplicative.*

*Proof.* Let $m$ and $n$ be coprime natural numbers. Let $d$ be a divisor of $n \cdot m$. Set $v = (d, n)$ and $w = \frac{d}{v}$. Then $(w, n) = 1$ and $w \mid n \cdot m$. Euclid's Lemma 0.4 implies $w \mid m$. In other words, every divisor $d$ of $m \cdot n$ can be written uniquely as $d = w \cdot v$ with $w \mid m$ and $v \mid n$.

$$\sigma(m\,n) = \sum_{d|mn} d = \sum_{w|m}\sum_{v|n} w\,v = \Big(\sum_{w|m} w\Big) \cdot \Big(\sum_{v|n} v\Big) = \sigma(m) \cdot \sigma(n)$$

$$\tau(m\,n) = \sum_{d|mn} 1 = \sum_{w|m}\sum_{v|n} 1 = \Big(\sum_{w|m} 1\Big) \cdot \Big(\sum_{v|n} 1\Big) = \tau(m) \cdot \tau(n) \qquad \square$$

This proof generalises to show that the function $\sigma_k(n) = \sum_{d|n} d^k$ is multiplicative for all real values of $k$. With this notation $\sigma = \sigma_1$ and $\tau = \sigma_0$. Again, neither is completely multiplicative.

**Theorem 2.4.** *Suppose that $n \in \mathbb{N}$ has the prime factorisation $n = \prod_{i=1}^{r} p_i^{a_i}$. Then*

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{a_i+1} - 1}{p_i - 1} \qquad \text{and} \qquad \tau(n) = \prod_{i=1}^{r} (a_i + 1).$$

*Proof.* Theorem 2.3 implies that $\sigma(n) = \prod_i \sigma\left(p_i^{a_i}\right)$. Let $p$ be a prime. The divisors of $p^k$ are $1, p, p^2, \ldots, p^k$. Hence $\sigma(p^k) = 1 + p + \cdots + p^k = \frac{p^{k+1}-1}{p-1}$. Similarly $\tau(n) = \prod_i \tau(p_i^{a_i})$ and $p^k$ has $k+1$ divisors. □

## 2.3 Möbius inversion

**Definition.** An integer $n > 1$ is *square-free* if it has no square divisors greater than 1.

**Lemma 2.5.** *i). An integer $n > 1$ is square-free if and only if it is a product of distinct primes.*

*ii). Every integer $n > 1$ can be written as $a \cdot b^2$ with $a$ square-free.*

*iii). Let $n > 1$ be a square-free integer and $m \in \mathbb{Z}$. If $p \mid m$ for all prime divisors $p$ of $n$, then $n$ divides $m$.*

*Proof.* i). $\Rightarrow$: Factor $n$ into its prime factorisation. If one prime $p$ arises to a higher power than 1, then $p^2$ divides $n$ which is impossible if $n$ is square-free. $\Leftarrow$: If $d^2$ divides a product of distinct primes, then the prime factorisation of $d$ can not contain any of those primes. Hence $d = 1$ and so $n$ is square-free.

ii). Let $n > 1$. Among all the squares dividing $n$, there is one that is the largest; call it $b^2$. Since it divides $n$, we find a $a \in \mathbb{N}$ such that $n = a \cdot b^2$. Now if $d^2$ divides $a$, then $d^2b^2$ divides $n$. But there is no larger square dividing $n$, hence $d^2b^2 = b^2$ shows that $d \leqslant 1$ and $a$ is square-free.

iii). As $n$ is square-free, we can write $n = p_1 \cdot p_2 \cdots p_r$ for distinct prime numbers $p_i$. Assume that $p_i$ divides $m$ for all $i$. Now apply Corollary 0.5 repeatedly to show that $n = p_1 \cdot p_2 \cdots p_r$ must divide $m$.

□

**Definition.** The *Möbius function* $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \text{ is not square-free} \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r \text{ with } p_i \text{ distinct primes.} \end{cases}$$

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | ... | 30 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mu(n)$ | 1 | $-1$ | $-1$ | 0 | $-1$ | 1 | $-1$ | 0 | 0 | 1 | $-1$ | 0 | | $-1$ |

**Lemma 2.6.** *If $n > 1$, then $\sum_{d|n} \mu(d) = 0$.*

**Example.** $\mu(12)+\mu(6)+\mu(4)+\mu(3)+\mu(2)+\mu(1) = 0+1+0+(-1)+(-1)+1 = 0$. ◇

*Proof.* Write $n = p_1^{a_1} \cdots p_r^{a_r}$. Then in the sum $\sum_{d|n} \mu(d)$ we can neglect all terms for which $d$ is not square-free.

$$\begin{aligned}
\sum_{d|n} \mu(d) &= \sum_{\substack{d|n \\ \text{square-free}}} \mu(d) \\
&= \mu(1) + \mu(p_1) + \mu(p_2) + \cdots + \mu(p_r) + \\
&\qquad + \mu(p_1p_2) + \mu(p_1p_3) + \cdots + \mu(p_{r-1}p_r) + \\
&\qquad + \mu(p_1p_2p_3) + \cdots + \mu(p_1p_2\cdots p_r) \\
&= 1 + r\cdot(-1)^1 + \binom{r}{2}(-1)^2 + \binom{r}{3}(-1)^3 + \cdots + \binom{r}{r}(-1)^r \\
&= (1+(-1))^r = 0
\end{aligned}$$

□

**Definition.** The *convolution* of two arithmetic functions $f$ and $g$ is defined by

$$(f * g)(n) = \sum_{d|n} f(d) \cdot g\left(\tfrac{n}{d}\right) = \sum_{de=n} f(d) \cdot g(e).$$

We define two auxiliary arithmetic functions $I$ and $\varepsilon$. They are defined by $I(n) = 1$ for all $n$ and

$$\varepsilon(n) = \begin{cases} 1 & \text{if } n = 1; \\ 0 & \text{if } n > 1. \end{cases}$$

**Lemma 2.7.** *For all arithmetic functions $f$, $g$, $h$:*

*i).* $(f * I)(n) = \sum_{d|n} f(d)$

*ii).* $f * g = g * f$

*iii).* $f * (g * h) = (f * g) * h$

*iv).* $I * \mu = \mu * I = \varepsilon$

*v).* $f * \varepsilon = \varepsilon * f = f$

*Proof.* The first property is by definition, the second follows from the symmetry of the formula $(f*g)(n) = \sum_{ed=n} f(e)g(d)$. The third property is shown as follows:

$$\begin{aligned}\Big(f * (g * h)\Big)(n) &= \sum_{ec=n} f(c) \cdot (g * h)(e) \\ &= \sum_{ec=n} f(c) \cdot \sum_{ab=e} g(a)h(b) \\ &= \sum_{abc=n} f(c) \cdot g(a) \cdot h(b)\end{aligned}$$

which is symmetric again, therefore it equals $\big((f * g) * h\big)(n)$ for all $n$. Property iv) is easy for $n = 1$ and is exactly what the previous lemma says for $n > 1$. The last property is easy again. □

**Theorem 2.8** (Möbius inversion Theorem)**.** *If $f$ is an arithmetic function and $F(n) = \sum_{d|n} f(d)$ then $f(n) = \sum_{d|n} \mu(d) \cdot F\big(\frac{n}{d}\big)$.*

*Proof.* $F = f * I$ implies $\mu * F = \mu * (f * I) = f * (\mu * I) = f * \varepsilon = f$. □

**Example.** By definition, we have $\sigma(n) = \sum_{d|n} d$. So the Möbius inversion theorem for $f(n) = n$ and $F(n) = \sigma(n)$ yields the formula

$$n = \sum_{d|n} \mu(d)\sigma\Big(\frac{n}{d}\Big).$$

For instance

$$\begin{aligned}12 &= \mu(12)\sigma(1) + \mu(6)\sigma(2) + \mu(4)\sigma(3) + \\ &\qquad + \mu(3)\sigma(4) + \mu(2)\sigma(6) + \mu(1)\sigma(12) \\ &= 0 \cdot 1 + (+1) \cdot 3 + 0 \cdot 4 + (-1) \cdot 7 + (-1) \cdot 12 + (+1) \cdot 28.\end{aligned}$$

◇

**Theorem 2.9.** *Let $f$ be an arithmetic function such that $f(1) = 1$. Then there exists a unique arithmetic function $g$ such that $f * g = \varepsilon$. The arithmetic function $g$ is called the* Dirichlet inverse *of $f$.*

*Proof.* We are looking for a function $g$ such that $\varepsilon(n) = (f * g)(n)$ for all $n$. For $n = 1$, this imposes that $1 = \varepsilon(1) = (f*g)(1) = f(1)\cdot g(1) = g(1)$. If $n = p$ is a prime, we find $0 = \varepsilon(p) = f(1) \cdot g(p) + f(p) \cdot g(1)$. This forces us to set $g(p) = -f(p)$. Similarly, one can show that we must have $g(p^2) = -f(p)^2 - f(p^2)$ by taking $n = p^2$. Now, we see that in general for an integer $n > 1$, the equations $(f * g)(n) = \varepsilon(n) = 0$ imposes us to set

$$g(n) = -\sum_{n \neq d | n} g(d) \cdot f\big(\frac{n}{d}\big).$$

if we already know the value of $g$ for all divisors $d$ of $n$. Hence, we construct inductively a unique function that satisfies $f * g = \varepsilon$. □

**Corollary 2.10.** *The set $G$ of all arithmetic functions $f$ with $f(1) = 1$ forms an abelian group under the convolution $*$ with $\varepsilon$ being the identity element.*

*Proof.* This is the summary of the previous theorem with parts ii), iii), v) of Lemma 2.7. □

**Example.** The Dirichlet inverse of $I$ is $\mu$ by part iv) of Lemma 2.7. What is Dirichlet inverse of $\tau$? We are looking for a function $g$ such that $\tau * g = \varepsilon$. We can write $\tau = I * I$ and solve the equation on $g$:

$$\begin{aligned}
I * I * g &= \varepsilon && \text{now } * \text{ by } \mu \text{ on the left} \\
\mu * I * I * g &= \mu * \varepsilon \\
\varepsilon * I * g &= \mu \\
I * g &= \mu && \text{and do it once more} \\
\mu * I * g &= \mu * \mu \\
\varepsilon * g &= \mu * \mu \\
g &= \mu * \mu.
\end{aligned}$$

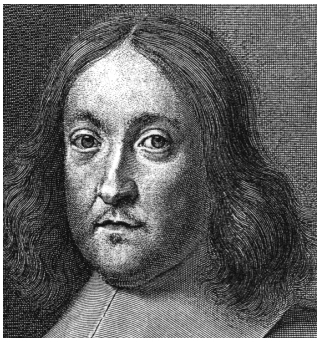
◇

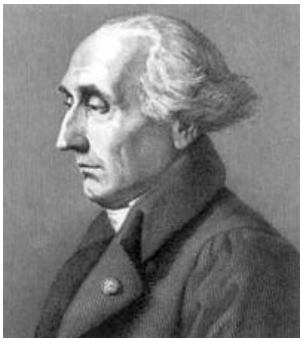
# 3 Basic theorems on primes

In this section, we will prove a few basic theorems on prime numbers. This will be applied to find primality testing and factorisation methods.

## 3.1 Fermat, Euler and Wilson

Some classic theorems in number theory. Proven by Pierre de Fermat (1601–1665), Leonhard Euler (1707 – 1783) and by Joseph-Louis Lagrange (1736–1813).





Lagrange gave the first proof to the following theorem, already stated without proof before by Ibn al-Haytham (c. 1000 AD), Edward Waring, and John Wilson.

**Theorem 3.1** (Wilson's Theorem)**.** *If $p$ is a prime, then* $(p-1)! \equiv -1 \pmod{p}$.

*Proof.* We may suppose that $p$ is odd as the theorem is true for $p = 2$. Each element of the group $(\mathbb{Z}/p\mathbb{Z})^*$ is represented exactly once in the product $(p-1)! = 1 \cdot 2 \cdots (p-1)$. For each $1 \leqslant a < p$ there is a unique $1 \leqslant b < p$ such that $a\,b \equiv 1 \pmod{p}$.

If $a = b$, then $a^2 \equiv 1 \pmod{p}$. This then implies that $p$ divides $a^2 - 1 = (a-1)(a+1)$, from which we deduce that $p$ divides $a-1$ or $a+1$ as $p$ is prime. Hence only $a = 1$ and $a = p-1$ are equal to their own inverses.

Therefore, every factor in the product $[2] \cdots [p-3] \cdot [p-2]$ cancels out with exactly another factor in the same product, without any overlaps. Hence

$$(p-1)! \equiv 2 \cdot 3 \cdots (p-2) \cdot (p-1) \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}. \qquad \square$$

**Example.** For $p = 11$, we get $10! = 3628800$, which is congruent to 10 modulo 11. Recall that the remainder of an integer modulo 11 can be computed as the alternating sum of its decimal digits. Here $0 - 0 + 8 - 8 + 2 - 6 + 3 = -1$. ◇

**Corollary 3.2.** *Let $p$ be an odd prime number. Then*

$$\Big(\big(\frac{p-1}{2}\big)!\Big)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

*Proof.* Starting from Wilson's Theorem, we have

$$\begin{aligned} -1 &\equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p} \\ &\equiv 1 \cdot 2 \cdot 3 \cdots \big(\tfrac{p-1}{2}\big) \cdot (-1) \cdot (-2) \cdot (-3) \cdots \big(-\tfrac{p-1}{2}\big) \pmod{p}. \end{aligned}$$

Now on the right hand side, we see two factors of $(\frac{p-1}{2})!$ and $(p-1)/2$ factors of $(-1)$. □

**Example.** It follows from this corollary that $\big((p-1)/2\big)!$ is $\pm 1$ modulo $p$ if $p \equiv 3 \pmod 4$, but it does not say which. Otherwise it is an element $i$ such that $i^2 \equiv -1 \pmod 4$. Here are the first few values

| $p$ | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $\big((p-1)/2\big)! \bmod p$ | 1 | 2 | −1 | −1 | 5 | 13 | −1 | 1 | 12 | 1 | 31 |

◇

**Theorem 3.3** (Fermat's little Theorem)**.** *If $p$ is a prime and $a$ is a positive integer with $p \nmid a$, then*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{3}$$

*Proof.* Since $p \nmid a$, the congruence class $[a]$ belongs to the group $(\mathbb{Z}/p\mathbb{Z})^*$. Hence the list $[a]$, $[2] \cdot [a]$, …, $[p-1] \cdot [a]$ also contains each non-zero congruence class exactly once. Therefore

$$\begin{aligned} a \cdot 2a \cdot 3a \cdots (p-1)\, a &\equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p} \\ a^{p-1} \cdot (p-1)! &\equiv (p-1)! \pmod{p} \end{aligned}$$

Since $(p-1)! \not\equiv 0 \pmod p$, we can simplify the above to equation (3). □

Alternatively, we may use group theory to prove it. Corollary 1.3.6 in G12ALN showed that the order of a group element divides the group order. Here $G = (\mathbb{Z}/p\mathbb{Z})^*$ is of order $p-1$. If $r$ is the order of $[a]$, then $p-1 = rk$ for some integer $k$. Now by definition $[a]^r = [1]$. Therefore $[a]^{p-1} = \big([a]^r\big)^k = [1]^k = [1]$ gives the above theorem again.

**Corollary 3.4.** *If $p$ is prime, then $a^p \equiv a \pmod{p}$, for every $a \in \mathbb{Z}$.*

*Proof.* If $p \nmid a$, then we obtain this by multiplying (3) by $a$ on both sides. If $p \mid a$, then $a^p \equiv 0 \equiv a \mod p$. □

**Theorem 3.5** (Euler's Theorem)**.** *Let $n$ be a positive integer, and $a \in \mathbb{Z}$ with $(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

This is a generalisation of Fermat's little Theorem 3.3 since $\varphi(p) = p-1$ if $p$ is prime. The proof is a generalisation, too.

*Proof.* Since $(a, n) = 1$, the congruence class $[a]$ belongs to the group of units $(\mathbb{Z}/n\mathbb{Z})^*$. Multiplying each element of $(\mathbb{Z}/n\mathbb{Z})^*$ by $[a]$ just permutes the group elements. We obtain

$$\prod_{x \in (\mathbb{Z}/n\mathbb{Z})^*} [a] \cdot x = \prod_{x \in (\mathbb{Z}/n\mathbb{Z})^*} x$$

$$[a]^{\varphi(n)} \cdot \prod_{x \in (\mathbb{Z}/n\mathbb{Z})^*} x = \prod_{x \in (\mathbb{Z}/n\mathbb{Z})^*} x$$

Simplifying on both sides by the product yields the desired congruence. □

Alternatively it is again a simple consequence of Corollary 1.3.6.

As explained above Fermat's little Theorem follows from knowing the group order of $\big(\mathbb{Z}/p\mathbb{Z}\big)^*$. Instead, we know actually much more:

**Theorem 3.6.** *Let $p$ be a prime. Then $\big(\mathbb{Z}/p\mathbb{Z}\big)^*$ is a cyclic group of order $p-1$.*

*Proof.* Theorem 2.5.3 in G12ALN. □

**Example.** For instance if $p = 19$, then $[13]$ is a generator of the cyclic group $(\mathbb{Z}/19\mathbb{Z})^*$ of order 18. We have

| $k$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $[13]^k$ | $[1]$ | $[13]$ | $[17]$ | $[12]$ | $[4]$ | $[14]$ | $[11]$ | $[10]$ | $[16]$ | $[18]$ | $[6]$ |
| $k$ | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| $[13]^k$ | $[2]$ | $[7]$ | $[15]$ | $[5]$ | $[8]$ | $[9]$ | $[3]$ | $[1]$ | $[13]$ | $[17]$ | $[12]$ |

The sequence starts to be period at $k = p-1$. Before that it seems to go randomly through the residue classes. This fact is used in cyptography (El Gamal cipher) for very large primes $p$. See G13CCR. ◇

**Definition.** Let $m$ be an integer such that $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$ is a cyclic group. An integer $g$ such that $[g]$ generates this cyclic group is called a *primitive element modulo $m$*.

Primitive elements exists modulo primes by the above theorem and modulo powers of odd primes (see G13FNT), but not for arbitrary modulus $m$. If there are, we can find one by trying the first few small integers using the following criterion.

**Proposition 3.7.** *Let $p$ be a prime and $a$ an integer which is not divisible by $p$. If $a^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{p}$ for all prime divisors $\ell$ of $p-1$, then $a$ is a primitive element.*

*Proof.* We know that $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ is a cyclic group by Theorem 3.6. Let $d$ be the order of the element $[a]$ in this group. By Lagrange's theorem (Corollary 1.3.6 in G12ALN), we know that $d$ divides $p-1$. We want to show that $d = p-1$.

Write $p - 1 = d \cdot e$. We have $a^d \equiv 1 \pmod{p}$. Suppose $e > 1$ and let $\ell$ be a prime factor of $e$. Then $d$ divides $\frac{p-1}{\ell}$, say $dk = \frac{p-1}{\ell}$. Therefore $a^{\frac{p-1}{\ell}} = a^{dk} \equiv 1 \pmod{p}$, which contradicts the hypothesis. Therefore $e = 1$ and $d = p - 1$. □

**Example.** We use this to check that 13 is a primitive element modulo $p = 19$: The prime factors of $p - 1 = 18$ are 2 and 3. So we have to compute $a^{\frac{p-1}{2}} = [13]^9$ and $a^{\frac{p-1}{3}} = [13]^6$. Since $[13]^9 = [-1]$ and $[13]^6 = [11]$, we see that 13 is indeed a primitive element. ◇

Here is a list of the smallest positive primitive element $g$ for the first few primes.

| $p$ | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 | 47 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $g$ | 1 | 2 | 2 | 3 | 2 | 2 | 3 | 2 | 5 | 2 | 3 | 2 | 6 | 3 | 5 |

**Aside:** *Artin's conjecture.* Is it true that 2 appears infinitely often in the above list? This is still an unsolved problem. Heath-Brown showed in 1986 that we have infinitely often a number below 8 in this list. ◇

## 3.2 Primality tests

In view of its application to cryptography (see G13CCR next year), one would like to the solve the following two problems effectively (say with a fast computer and huge, huge entries): Given an integer $n > 1$, can we decide if $n$ is prime or composite? Given an integer $n > 1$, can we find its prime factorisation?

**Theorem 3.8** (Trial division)**.** *If $n \in \mathbb{Z}$ is composite, then $n$ has a prime factor not exceeding $\sqrt{n}$.*

*Proof.* Since $n$ is composite, there are $a, b \in \mathbb{Z}$ such that $1 < a \leqslant b < n$ and $n = a\,b$. We have $a \leqslant \sqrt{n}$ because $a^2 \leqslant a\,b = n$. Now $a$ has a prime divisor $p$, which divides $n$, too, and $p \leqslant a \leqslant \sqrt{n}$. □

If we have a list of all the primes $p$ below $10^6$, then by this theorem we have an efficient way to solve both questions for $n < 10^{12}$. Just try to divide $n$ by all primes in the list. If none divides $n$, then $n$ is prime. Otherwise, we can divide $n$ by $p$ and try to divide $\frac{n}{p}$ and so forth until we get the full factorisation of $n$. To store all 37607912018 primes below $10^{12}$ would take more then 168 GB. Trial division is not efficient for $n$ with hundreds or thousands of digits.

The following is a converse to Wilson's Theorem 3.1.

**Proposition 3.9.** *If $n$ is a positive integer such that $(n-1)! \equiv -1 \pmod{n}$, then $n$ is prime.*

*Proof.* Suppose $n = ab$ with natural number $a$ and $b$. If $a$ and $b$ are both smaller than $n$, then $a$ and $b$ appear in $(n-1)!$ and so $n = ab$ divides $(n-1)!$. But then $0 \equiv (n-1)! \equiv -1 \pmod{n}$. So $a$ or $b$ must be equal to $n$ the other 1. □

This proposition would give another method of decide if $n$ is prime. However, it is useless as it would take long to compute $(n-1)!$ modulo $n$. It is a bit of a surprise that the following is a rather efficient test to prove that an integer $n$ is composite.

**Proposition 3.10.** *Let $n > 1$. Suppose $b$ is coprime to $n$ and that $b^{n-1} \not\equiv 1 \pmod{n}$, then $n$ is composite.*

*Proof.* This is the contra-positive of Fermat's little Theorem 3.3. □

**Example.** For instance, we can prove that 15 is composite: Take $b = 2$, then $2^{14} = 16384 \equiv 4 \pmod{15}$. This tells us that 15 is composite without revealing any factors. ◇

How do we compute $a^k$ modulo $n$? The naive way is to evaluate $a^k$ and then to take the remainder modulo $n$. But that takes at least $k$ steps and involves huge integers. It is better to reduce modulo $n$ after each multiplication; however that still involves $k$ steps. For $k = n-1$ this is worse than trial division. So here is the idea to compute this, it is called *fast modular exponentiation*:

Write $k$ in binary expansion

$$k = k_r \cdot 2^r + k_{r-1} \cdot 2^{r-1} + \cdots + k_1 \cdot 2 + k_0 \,.$$

By definition $k_r = 1$. Start with $b = a$. Now, if $k_{r-1}$ is 1, then we replace $b$ by $a \cdot b^2$ modulo $n$, otherwise by $b^2$ modulo $n$. Then with the same rule for $k_{r-2}$ and so on. In the end $b$ will have the value $a^k$ modulo $n$. The idea is simply the following equation

$$a^k = a^{k_0} \cdot \left( a^{k_1} \cdot \left( a^{k_2} \left( \cdots \left( a^{k_{r-1}} \cdot (a^{k_r})^2 \right)^2 \cdots \right)^2 \right)^2 \right)^2 .$$

So all we need to do is squaring $r$ times and maybe multiplying a few times by $a$, always modulo $n$. We can represent this in a simple table

| $i$ | $r$ | $r-1$ | $\ldots$ | $1$ | $0$ | |
|---|---|---|---|---|---|---|
| $k_i$ | $1$ | $k_{r-1}$ | $\ldots$ | $k_1$ | $k_0$ | $\leftarrow$ fill in the binary digits of $k$ |
| $b$ | $a$ | $\ldots$ | $\ldots$ | | | $\leftarrow$ fill up from the left, each step either $a \cdot b^2$ or $b^2$ modulo $n$ |

Since $r \leqslant \log_2(n)$ this method uses at most $2 \cdot \log_2(n)$ operations. When $n$ is large this is much better than $n$ or $\sqrt{n}$.

**Example.** For instance suppose we want to compute $3^{220}$ modulo $n = 221$. As $220 = 2^7 + 2^6 + 2^4 + 2^3 + 2^2 = 11011100_2$, we get

| $i$ | 7 | 6 | 5 | 4 |
|---|---|---|---|---|
| $k_i$ | 1 | 1 | 0 | 1 |
| $b$ | 3 | $3 \cdot 3^2 \equiv 27$ | $27^2 \equiv 66$ | $3 \cdot 66^2 \equiv 29$ |

| $i$ | 3 | 2 | 1 | 0 |
|---|---|---|---|---|
| $k_i$ | 1 | 1 | 0 | 0 |
| $b$ | $3 \cdot 29^2 \equiv 92$ | $3 \cdot 92^2 \equiv 198$ | $198^2 \equiv 87$ | $87^2 \equiv 55$ |

So $3^{220} \equiv 55 \pmod{221}$. It proves that 221 is composite. This is much better than passing through the computation of $3^{220}$, which has 105 decimal digits. ◇

**Example.** For example consider the integer

$$\begin{aligned} n =& 2405103478365565317102362319979107852729856194163135049\ldots \\ & \ldots 85366876371679159591228139692810023115202389185249377 9 \end{aligned}$$

Trial division will never (well, at least not in within the age of the universe) succeed in deciding if $n$ is prime or composite. On the other hand, my computer in the office takes about 50 $\mu s$ to evaluate

$$\begin{aligned} 2^{n-1} \equiv& 158256580117107554768470787587371196902955183533611778\ldots \\ & \ldots 99830177713682596744025238851645525800682821028774844 5 \end{aligned}$$

modulo $n$. Hence $n$ is not prime. Yet, we have not idea what the prime factors are. ◇

**Aside:** *Fast modular exponentiation* Here is the code for an alternative version of fast modular exponentiation. Rather then reading teh binary digits from left-to-right, this reads them from right-to-left. In fact, it computes these digits as we go along.

```
def modexp(a,k,n):
    r = 1
    b = a
    while k > 0:
        if k is odd:
            r = r*b mod n
        b = b^2 mod n
        k = k//2
    return r
```

◇

Note that the converse to Proposition 3.10 is not valid. For instance $11^{14} \equiv 1 \pmod{15}$ does not imply that 15 is prime. With respect to the base $b = 11$, the composite number $n = 15$ behaves like a prime.

**Definition.** Let $n > 1$. If $b^{n-1} \equiv 1 \pmod{n}$ yet $n$ is composite, then $n$ is called a *pseudoprime to base b*. A composite number $n$ that is pseudoprime to all bases $b > 1$ with $(b, n) = 1$ is called a *Carmichael number*.

**Theorem 3.11.** *Suppose $n > 1$ is a square-free composite number such that $(p-1) \mid (n-1)$ for all primes $p$ dividing $n$. Then $n$ is a Carmichael number.*

*Proof.* Let $b > 1$ be an integer coprime to $n$. Let $p \mid n$. Then $b$ is coprime to $p$. By assumption there is an integer $t$ such that $n - 1 = t \cdot (p-1)$. By Fermat's Little Theorem 3.3, $b^{n-1} = (b^t)^{p-1} \equiv 1 \pmod{p}$. Therefore $p$ divides $b^{n-1} - 1$ for all prime divisors of $n$. By the third part of Lemma 2.5 the assumption that $n$ is square-free implies that $n$ divides $b^{n-1} - 1$. □

**Example.** Let $n = 561$. The prime factorisation of $n$ is $3 \cdot 11 \cdot 17$. Now $3 - 1$ divides $561 - 1$, also $11 - 1$ divides it and $17 - 1$ does. Hence 561 is a Carmichael number. The theorem shows that $b^{560} \equiv 1 \pmod{561}$ for all $b$ with $(b, 561) = 1$. ◇

**Aside:** 561 is the smallest Carmichael number. The following are 1105, 1729, 2465, 2821, 6601... (for a longer list see `http://oeis.org/A002997`). Even worse, it is known that there are infinitely many of them (Red Alford, Andrew Granville and Carl Pomerance in 1994). Therefore one needs stronger methods to prove that a suspected huge number is indeed prime. Some examples are Pocklington's test, elliptic curve primality test, Agrawal-Kayal-Saxena primality test. At worst it takes something like $\log(n)^6$ steps to check if $n$ is prime.

In contrast, factorisation is much harder. The following is a simple method, which is quite a bit faster than the above trial division. However, one does not expect that it could be done in time polynomial in $\log(n)$; except on a quantum computer. ◇

## 3.3 Pollard $p - 1$ factorisation

Let $n$ be an integer. Think of an integer with 20 to 50 decimal digits. We want to find the prime factorisation of $n$. Note that it is enough to

find one divisor $1 < d < n$ of $n$ for we could then apply our method recursively for the smaller numbers $d$ and $\frac{n}{d}$.

We will certainly start by using trial division to see if $n$ is divisible by 2, 3, 5, 7, etc. On a computer, we could test to divide by all prime numbers up to $10^6$ in no time. So we may assume that $n$ has no small prime factor, in particular it is certainly an odd number. Also, we would check with a fast test to see if $n$ is composite or prime. Therefore, we will also assume that $n$ is composite.

First assume, a gentle fairy comes to help us. She gives us a number $K$ and tells us that there is a prime factor $p$ of $n$ such that $p-1$ divides $K$. However she does not tell us what $p$ is.

Now, we pick a random $1 < a < n$. If $(a, n)$ is not 1, then we have a factor, so we may assume that $(a, n) = 1$. Now compute $a^K - 1$. Because the fairly told us that there is an integer $t$ such that $(p-1)t = K$, we find

$$a^K \equiv a^{t(p-1)} = (a^t)^{p-1} \equiv 1 \pmod{p}$$

which shows that $p$ divides $a^K - 1$. Hence $p$ divides $(a^K - 1, n)$. One of two things can happen: Either this gcd is a proper divisor of $n$ and we are done, or $(a^K - 1, n) = n$. In the latter case, we just pick another $a$ and hope we are not unlucky again.

**Example.** Say $n = 121933417163$. The fairy tells us that

$$K = 32176447673406729078990845541 30$$

has the good property. Indeed taking $a = 2$, we find that $(a^K - 1, n) = 987659$. This happens to be the bigger of the two prime factors of $n$. $\diamond$

The example should alert us. It looks like computing $a^K$ is going to be very tedious with such large values of $K$. However, we only need to compute $a^K$ modulo $n$, since we will take the gcd with $n$ afterwards. This can be done very fast even for huge $K$ and $n$.

Now, the real problem about this world is that fairies hardly ever help us. So how would we get a good candidate for $K$? Let $B$ be an integer, say 100 or 1000. Then one first choice of $K$ would be to take the product of all prime numbers $\ell$ smaller than $B$. In fact that is $K$ in the example above with $B = 80$. Now this $K$ will work if one prime factor $p$ of $n$ is such that $p-1$ factors into a product of distinct primes $\ell$ all smaller than $B$. In the example above $p - 1 = 987658 = 2 \cdot 7 \cdot 19 \cdot 47 \cdot 79$ had this property.

A slightly better version takes smaller primes $\ell$ to some powers. For instance it is rather likely that $p-1$ is divisible by 4. A typical $K$ is the

product $K = \prod \ell^{n_\ell}$ such that $\ell^{n_\ell}$ is the largest power of $\ell$ which is just smaller than $B$. If $p-1$ divides this $K$, it is called $B$-power-smooth.

As a summary here the method explained again. We want to factor $n$.

- Pick a bound $B$ (best not with more than 6 decimal digits).
- Compute $K$ as a product over all primes $\ell < B$ of the largest prime power $\ell^{n_\ell} < B$.
- Pick an integer $1 < a < n$. If $(a, n) > 1$, then we found a factor of $n$ and stop.
- Compute $d = (a^K - 1, n)$ using fast modular exponentiation.
  - If $1 < d < n$, then we found a factor of $n$.
  - If $d = 1$, then the choice of $B$ was too small. Increase it.
  - If $d = n$, we try some other values of $a$ or decrease $B$.

**Example.** As a toy example, we wish to factor $n = 6887$. We pick $B = 5$. Then $K = 2^2 \cdot 3 \cdot 5 = 60$. Then $2^{60} - 1 \equiv 1961$ modulo $n$. But $(1961, n) = 1$.

Now, we increase $B$ to 7. We get $K = 2^2 \cdot 3 \cdot 5 \cdot 7 = 420$. Then $2^{420} - 1 \equiv 1917 \pmod{n}$. Now $(1917, n) = 71$ and we have found a factor of $n$. ◇

**Aside:** *H*ow likely is it that $p-1$ is $B$-power-smooth for some given $B$? In Figure 3 we see a plot of the percentage for some values of $B$.

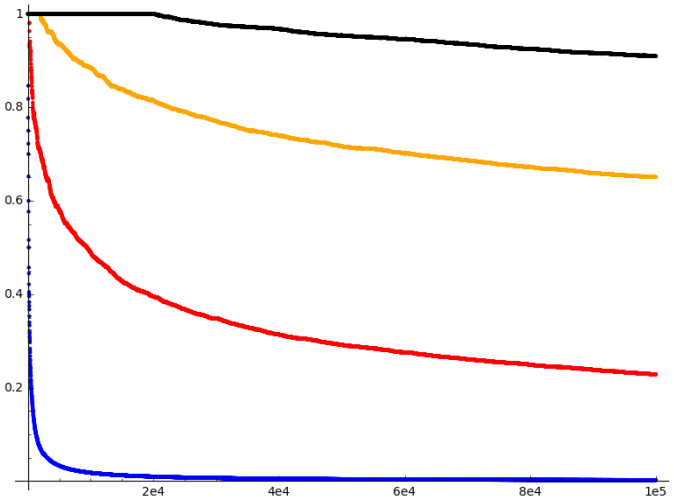



Figure 3: The proportion of primes up to 100000 that are such that $p-1$ is $B$-power-smooth for $B = 10$, 100, 1000 and 10000.

◇

# 4 Quadratic Reciprocity

We will answer in this chapter how to solve equations like $x^2 \equiv a \pmod{p}$ for a prime $p$. In fact, that is an exaggeration: We will only learn how to detect whether or not this equation has a solution.

Note that the question is without interest when $p = 2$. We will therefore assume throughout this chapter that $p$ is an *odd* prime.

For $p = 3$, we see that $x^2 \equiv 2$ has no solution, since $0^2 \equiv 0$ and $1^2 \equiv (-1)^2 \equiv 1$. For $p = 5$, we can compute all squares:

| $x$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $x^2$ | 0 | 1 | 4 | 4 | 1 |

So only when $a \equiv 0, 1, 4 \pmod{5}$, we have a solution to $x^2 \equiv a \pmod{p}$. Similarly for $p = 7$, we have

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $x^2$ | 0 | 1 | 4 | 2 | 2 | 4 | 1 |

so only $a \equiv 0, 1, 2, 4$ admit a "square root", but not $a \equiv 3, 5, 6$.

## 4.1 The Legendre symbol

**Definition.** A *quadratic residue* modulo $p$ is an integer $a \pmod{p}$ such that $p \nmid a$ and $x^2 \equiv a \pmod{p}$ has solutions; a *quadratic non-residue*[1] modulo $p$ is an integer $a$ such that $p \nmid a$ and $x^2 \equiv a \pmod{p}$ has no solutions.

**Lemma 4.1.** *Let $p$ be an odd prime. Let $g$ be a primitive element modulo $p$. Then $a \equiv g^k \pmod{p}$ is a quadratic residue if and only if $k$ is even, otherwise it is a quadratic non-residue. There are exactly $\frac{p-1}{2}$ quadratic residues modulo $p$ and just as many quadratic non-residues.*

*Proof.* If $k = 2n$ is even, then $x = g^n$ is a solution to $x^2 \equiv g^k \pmod{p}$ and hence $g^k$ is a quadratic residue. Conversely, if $b = g^n$ is a solution to $x^2 \equiv g^k \pmod{p}$ then $2n \equiv k \pmod{p-1}$. Since $p - 1$ is even, $k$ must be even, too.

Now, $g^0, g^2, g^4, \ldots, g^{p-3}$ are all quadratic residues modulo $p$ and $g^1$, $g^3$, $g^5, \ldots$, $g^{p-2}$ are all quadratic non-residues modulo $p$. There are $\frac{p-1}{2}$ of each. □

This would be false if $p$ were not assumed to be prime. The only invertible residue classes that are square modulo 15 are 1 and 4.

**Definition.** The *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined for $a \in \mathbb{Z}$ and $p$ an odd prime by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a; \\ +1 & \text{if } p \nmid a \text{ and } x^2 \equiv a \pmod{p} \text{ has solutions;} \\ -1 & \text{if } p \nmid a \text{ and } x^2 \equiv a \pmod{p} \text{ has no solutions.} \end{cases}$$

So $\left(\frac{a}{p}\right) = +1$ when $a$ is a quadratic residue and $\left(\frac{a}{p}\right) = -1$ when $a$ is a quadratic non-residue modulo $p$.

Please write the () around $\frac{a}{p}$ to distinguish it from the fraction. A short way to define the Legendre symbol is to say that the number of solutions to $x^2 \equiv a \pmod{p}$ is $1 + \left(\frac{a}{p}\right)$.

**Proposition 4.2.** *i).* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ *when* $a \equiv b \pmod{p}$*;*

*ii).* Euler's Criterion: $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$*;*

*iii).* $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} +1 & \text{if } p \equiv 1 \pmod{4}; \\ -1 & \text{if } p \equiv 3 \pmod{4}; \end{cases}$

*iv).* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

*Proof.* i). Clear as the definition only depended on $a$ modulo $p$.

ii). If $p \mid a$, then both sides are zero modulo $p$.

Otherwise $a \equiv g^k$ for some $k$, where $g$ is a fixed primitive element modulo $p$. Now $\left(\frac{a}{p}\right) = (-1)^k$ by Lemma 4.1. Let $h = g^{(p-1)/2}$. Since $h^2 = g^{p-1} \equiv 1$ by Fermat's little Theorem 3.3, but $h \not\equiv 1 \pmod{p}$, we have $h \equiv -1 \pmod{p}$. Now $a^{(p-1)/2} \equiv h^k \equiv (-1)^k$ modulo $p$.

iii). Take $a = -1$ in the previous part. We find that $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}$. However both sides of this congruence are either $+1$ or $-1$. Since $p$ is odd, the two sides must be equal.

iv). Part ii) shows that

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2} \cdot b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

As both sides are among $-1, 0, 1$, this congruences is an equality. □

**Corollary 4.3.** *Let $p$ be an odd prime. The map $(\frac{\cdot}{p})\colon (\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\}$ is a group homomorphism.*

**Example.** In principle, Euler's criterion give a way to compute $(\frac{a}{p})$. But it is hardly faster than checking all residue classes $x$ for a solution to $x^2 \equiv a \pmod{p}$. For $p = 11$, we get

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $a^5$ | 1 | 32 | 243 | 1024 | 3125 | 7776 | 16807 | 32768 | 59049 | 100000 |
| $a^5 \bmod 11$ | 1 | $-1$ | 1 | 1 | 1 | $-1$ | $-1$ | $-1$ | 1 | $-1$ |
| $(\frac{a}{11})$ | 1 | $-1$ | 1 | 1 | 1 | $-1$ | $-1$ | $-1$ | 1 | $-1$ |

◇

**Aside:** *Primality testing using Euler's criterion.* Note that Euler's criterion is false when $p$ is not a prime. For instance is $2^7 \not\equiv \pm 1$ modulo 15 so 15 can not be a prime. More convincingly, $3^{1996001} \equiv 2664001 \not\equiv \pm 1 \pmod{3992003}$. So 3992003 is not prime.

A composite integer $n > 1$ is called an Euler pseudoprime to the base $b$ if $b^{(n-1)/2} \equiv \pm 1$. There are much fewer integers that are Euler pseudoprime to all bases $b > 1$ with $(b, n) = 1$. So this forms a much better test to prove that an integer $n$ is composite.

After extending the Legendre symbol to the Jacobi symbol $(\frac{a}{n})$ for any odd integer $n$, one can even test for $b^{(n-1)/2} \equiv (\frac{b}{n}) \pmod{n}$. ◇

An important consequence of the last item in Proposition 4.2 is the following. If we want to know how to evaluate $(\frac{a}{p})$ for all $a$, it is enough to evaluate $(\frac{-1}{p})$, $(\frac{2}{p})$ and $(\frac{q}{p})$ for odd primes $q$, as we can first factor $a$. For instance

$$\left(\frac{-2143018}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) \cdot \left(\frac{101}{p}\right) \cdot \left(\frac{103^2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) \cdot \left(\frac{101}{p}\right).$$

We will now proceed to give a formula for exactly the other two Legendre symbols $(\frac{2}{p})$ and $(\frac{q}{p})$. But first we not an interesting consequence of the above proposition.

**Theorem 4.4.** *There are infinitely many primes of the form $4n+1$.*

*Proof.* Suppose $\{p_1, \dots p_r\}$ is the complete list of primes of the form $4n+1$. Let $p$ be a prime divisor of $n = (2p_1 \cdots p_r)^2 + 1$. Then $-1$ is a quadratic residue modulo $p$, so $p \equiv 1 \pmod 4$. But $p$ can not be equal to $p_i$. Contradiction. □

**Aside:** As mentioned earlier, G13FNT will generalise this vastly and also explain in what sense roughly half of the primes are congruent to 1 modulo 4. ◇

## 4.2 The Computation of $(\frac{2}{p})$

We wish to find a closed formula for $(\frac{2}{p})$ only depending on the odd prime $p$. Here is what the first few values look like

| $p$ | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 27 | 31 | 37 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $(\frac{2}{p})$ | $-1$ | $-1$ | 1 | $-1$ | $-1$ | 1 | $-1$ | 1 | $-1$ | 1 | $-1$ |

**Definition.** Let $a$ be an integer. The integer $s$ such that $s \equiv a \pmod p$ and $|s| < \frac{p}{2}$ is called the *least residue* of $a$ modulo $p$.

**Proposition 4.5.** $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} +1 & \text{if } p \equiv \pm 1 \pmod 8; \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$

*Proof.* Let us start by proving the second equality: Write $p = 8k + i$ for some $i \in \{1, 3, 5, 7\}$. Now $p^2 - 1 = (8k+i)^2 - 1 = 64k^2 + 16k\,i + i^2 - 1 \equiv i^2 - 1 \pmod{16}$ is divisible by 16 if $i = 1$ or 7, but only divisible by 8 is $i = 3$ or 5.

Now to the first equality. Consider the least residues of all even integers $2, 4, \dots, p-1$.

$$\begin{aligned} p-1 \equiv -1 &\equiv (-1)^1 \cdot 1 \\ 2 \equiv \quad 2 &\equiv (-1)^2 \cdot 2 \\ p-3 \equiv -3 &\equiv (-1)^3 \cdot 3 \\ \vdots \quad &\vdots \qquad\quad \vdots \end{aligned}$$

There are $\frac{p-1}{2}$ elements in the list. Their product gives

$$2^{\frac{p-1}{2}} \cdot \Big(\frac{p-1}{2}\Big)! \equiv (-1)^{\frac{1}{2}\cdot\frac{p-1}{2}\cdot\frac{p+1}{2}} \cdot \Big(\frac{p-1}{2}\Big)! \pmod{p},$$

since $1+2+3+\cdots+\frac{p-1}{2} = \frac{1}{2}(\frac{p-1}{2})(\frac{p-1}{2}+1) = \frac{p^2-1}{8}$. Simplifying by the factorial on both sides and using Euler's criterion proves the proposition. □

## 4.3 The Law of Quadratic Reciprocity

**Theorem 4.6** (Law of Quadratic Reciprocity)**.** *Let $p$ and $q$ be distinct odd primes. Then*

$$\textit{i).}\ \Big(\frac{-1}{p}\Big) = (-1)^{(p-1)/2} = \begin{cases} +1 & \text{if } p \equiv 1 \pmod 4; \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

$$\textit{ii).}\ \Big(\frac{2}{p}\Big) = (-1)^{(p^2-1)/8} = \begin{cases} +1 & \text{if } p \equiv \pm 1 \pmod 8; \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

$$\textit{iii).}\ \Big(\frac{p}{q}\Big)\Big(\frac{q}{p}\Big) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} +1 & \text{if } p \equiv 1 \pmod 4 \textbf{ or } q \equiv 1 \pmod 4; \\ -1 & \text{if } p \equiv 3 \pmod 4 \textbf{ and } q \equiv 3 \pmod 4. \end{cases}$$

We have seen part i) and part ii) already. We will prove the most difficult part iii) later.

### Computation of Legendre symbols

Here an example of how to compute Legendre symbols very fast.

$$\begin{aligned}\Big(\frac{44}{47}\Big) &= \Big(\frac{4}{47}\Big)\cdot\Big(\frac{11}{47}\Big) = \Big(\frac{11}{47}\Big) = -\Big(\frac{47}{11}\Big) \\ &= -\Big(\frac{3}{11}\Big) = (-1)\cdot(-1)\cdot\Big(\frac{11}{3}\Big) = \Big(\frac{2}{3}\Big) = -1\end{aligned}$$

or faster

$$\Big(\frac{44}{47}\Big) = \Big(\frac{-3}{47}\Big) = \Big(\frac{-1}{47}\Big)\cdot\Big(\frac{3}{47}\Big) = (-1)\cdot(-1)\cdot\Big(\frac{47}{3}\Big) = \Big(\frac{2}{3}\Big) = -1$$

**Aside:** *Is the computation as slow as factorisation?* It is very quick to compute $(\frac{1000003}{3000017})$ this way, knowing that both entries are primes here. Otherwise we would have to factor and that may be very time consuming for large integers. Luckily there is a generalisation of Legendre symbols called Kronecker

symbols (or Jacobi symbols) which satisfy a quadratic reciprocity even for composite numbers.

So a computer can decide in milliseconds if a given integer $a$ is a quadratic residue modulo a huge prime $p$. ◇

## 4.4 Primes for which $a$ is a quadratic residue

The quadratic reciprocity law has an amazing consequence. We now fix $a$ and vary $p$.

**Proposition 4.7.** *Fix an integer $a > 1$. The set of all primes $p$ for which $(\frac{a}{p}) = +1$ consists of all primes in certain congruence classes modulo $4|a|$.*

For instance if $a = q$ is a prime which is congruent to $+1$ modulo 4. Then $(\frac{q}{p}) = (\frac{p}{q})$ by iii). The later only depends on the residue class of $p$ modulo $q = a$.

**Example.** As an example, we can take $a = 5$. Then 5 is a quadratic residue modulo $p$ if and only if $(\frac{p}{5}) = +1$. That is the case exactly when $p \equiv 1$ or 4 modulo 5.

| $p$ | 3 | 5 | 7 | 11 | 13 | 17 | 19 |
|---|---|---|---|---|---|---|---|
| $(\frac{5}{p})$ | $-1$ | 0 | $-1$ | 1 | $-1$ | $-1$ | 1 |
| $p \bmod 5$ | 3 | 0 | 2 | 1 | 3 | 2 | 4 |

◇

If instead $a = q$ is a prime which is congruent to 3 modulo 4. Then $(\frac{q}{p}) = \pm(\frac{p}{q})$ with the sign $+1$ if and only if $p \equiv +1 \pmod 4$. So we have that

$$\left(\frac{q}{p}\right) = +1 \Leftrightarrow \begin{cases} \left((\frac{p}{q}) = +1 \text{ and } p \equiv +1 \pmod 4\right) \text{ or} \\ \left((\frac{p}{q}) = -1 \text{ and } p \equiv -1 \pmod 4\right). \end{cases}$$

The first condition in both cases is a condition on $p$ modulo $q$ while the second is a condition on $p$ modulo 4. So by the Chinese remainder theorem, we can reformulate one condition modulo $4q$.

**Example.** As an example, we can take $a = 3$. The above shows that 3 is a quadratic residue modulo $p$ if and only if either $\big(p \equiv +1 \pmod 3$ and $p \equiv 1 \pmod 4\big)$ or $\big(p \equiv -1 \pmod 3$ and $p \equiv -1 \pmod 4\big)$. That is equivalent to either $p \equiv 1 \pmod{12}$ or $p \equiv -1 \pmod{12}$ by the Chinese remainder theorem.

| $p$ | 3 | 5 | 7 | 11 | 13 | 17 | 19 |
|---|---|---|---|---|---|---|---|
| $(\frac{3}{p})$ | 0 | $-1$ | $-1$ | 1 | 1 | $-1$ | $-1$ |
| $p \bmod 12$ | 0 | 5 | 7 | $-1$ | 1 | 5 | 7 |

$\diamond$

*Proof of Proposition 4.7.* We may assume that $a > 0$ is square-free or $-a > 0$ is square-free as square factors in $a$ can be neglected. Factor $a = \pm q_1 q_2 \cdots q_r$. Suppose we know what congruence class modulo $4|a|$ the prime $p$ belongs to. Then we know what congruence class modulo $4q_i$ it belongs to for all $i$. Hence we know the value of $(\frac{q_i}{p})$ by the above explanation in the two cases. We also know $(\frac{-1}{p})$. If $2 \mid a$, then $8 \mid 4a$; therefore we also know $(\frac{2}{p})$. Hence we know $(\frac{a}{p}) = (\frac{\pm 1}{p}) \cdot (\frac{q_1}{p}) \cdots (\frac{q_r}{p})$. $\square$

**Example.** We evaluate $(\frac{10}{p})$ as a further example with a composite $a$. We take $p \notin \{2, 5\}$, since $(\frac{10}{5}) = 0$. Note that $(\frac{10}{p}) = (\frac{2}{p})(\frac{5}{p})$; we evaluate the two factors separately, using quadratic reciprocity in each case.

First, since $5 \equiv 1 \pmod 4$ we have

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \begin{cases} +1 & \text{if } p \equiv \pm 1 \pmod 5, \\ -1 & \text{if } p \equiv \pm 2 \pmod 5. \end{cases}$$

Next, the value of $(\frac{2}{p})$ depends on $p \pmod 8$:

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{if } p \equiv \pm 1 \pmod 8, \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

Hence the product $(\frac{10}{p}) = (\frac{2}{p})(\frac{5}{p})$ depends on $p$ modulo 40. We get $(\frac{10}{p}) = +1$ if either $(\frac{2}{p}) = (\frac{5}{p}) = +1$ or $(\frac{2}{p}) = (\frac{5}{p}) = -1$. In other words $(\frac{10}{p}) = +1$ if either

$$p \equiv \pm 1 \pmod 8 \quad \text{and} \quad p \equiv \pm 1 \pmod 5$$

or

$$p \equiv \pm 3 \pmod 8 \quad \text{and} \quad p \equiv \pm 2 \pmod 5.$$

We use the Chinese Remainder Theorem to replace each pair ($p \bmod 5, p \bmod 8$) by a single class ($p \bmod 40$). For example,

$$\left\{ \begin{array}{ll} p \equiv 2 & \pmod 5 \\ p \equiv 3 & \pmod 8 \end{array} \right\} \iff p \equiv -13 \pmod{40}.$$

Combining all the possibilities in this way gives

$$\left(\frac{10}{p}\right) = +1 \iff p \equiv \pm 1, \pm 3, \pm 9, \pm 13 \pmod{40}.$$

The other residue classes modulo 40 (and coprime to 40) give the other cases:

$$\left(\frac{10}{p}\right) = -1 \iff p \equiv \pm 7, \pm 11, \pm 17, \pm 19 \pmod{40}.$$

Hence finally,

$$\left(\frac{10}{p}\right) = \begin{cases} +1 & \text{if } p \equiv \pm 1, \pm 3, \pm 9, \pm 13 \pmod{40}, \\ -1 & \text{if } p \equiv \pm 7, \pm 11, \pm 17, \pm 19 \pmod{40}. \end{cases}$$

◇

**Example.** Further examples that you are encouraged to compute in a similar way are the following three statements:

$$\left(\frac{6}{p}\right) = \begin{cases} +1 & \text{if } p \equiv \pm 1, \pm 5 \pmod{24}, \\ -1 & \text{if } p \equiv \pm 7, \pm 11 \pmod{24}. \end{cases}$$

$$\left(\frac{-5}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1, 3, 7, 9 \pmod{20}, \text{ and} \\ -1 & \text{if } p \equiv -1, -3, -7, -9 \pmod{20}. \end{cases}$$

$$\left(\frac{-3}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1 \pmod{3}; \\ -1 & \text{if } p \equiv 2 \pmod{3}. \end{cases}$$

In the last example with $a = -3$, one initially finds a condition modulo $4|a| = 12$. However it simplifies to a condition modulo 3. The same will be true for all $a = -q$ with $q$ a prime congruent to 3 modulo 4. ◇

**Aside:** More generally. Given a quadratic polynomial, like $x^2 - a$, then to know if the polynomial has a root modulo $p$ only depends on the congruence class of $p$ modulo some $m$. The same is no longer true for cubic polynomials. For instance, the polynomial $x^3 - 2$ has a solution modulo $p$ if and only if $p \equiv 2 \pmod 3$ or $\big(p \equiv 1 \pmod 3$ and $p = a^2 + 27b^2$ for some integers $a$ and $b\big)$. The last condition is not a condition modulo $m$ for any $m$. Examples of such primes are 31, 43, 109, 127, ... Behind all this is that a certain "Galois group" is no longer abelian. ◇

## 4.5 The proof of the quadratic reciprocity law

This is one of the many proofs of the quadratic reciprocity law. It is was discovered by G. Rousseau.

Let $p$ and $q$ be two distinct odd primes. We will consider the abelian group $G = \big(\mathbb{Z}/p\mathbb{Z}\big)^* \times \big(\mathbb{Z}/q\mathbb{Z}\big)^*$. It contains the normal subgroup $N = \big\{([1],[1]),([-1],[-1])\big\}$ of order 2. To ease the notation, we will write $(a,b)$ instead of $([a],[b])$. Each coset in $G/N$ consist of a pair of the form

$$(a,b)N = \Big\{(a,b),\ (-a,-b)\Big\}.$$

One of the two can be written with $1 \leqslant a \leqslant (p-1)/2$.

**Example.** Let's list the elements of the group $G/N$ for $p = 5$ and $q = 7$:

$$\begin{array}{cccccc} (1,1)N & (1,2)N & (1,3)N & (1,4)N & (1,5)N & (1,6)N \\ (2,1)N & (2,2)N & (2,3)N & (2,4)N & (2,5)N & (2,6)N \end{array}$$

The product of the first line is $(1,6!)N = (1,-1)N$ and for the second line it is $(2^6, 6!) = (-1,-1)$. So the product over all elements is $(-1,1)N = \{(-1,1),(1,-1)\}$. ◇

We will now compute the product of all elements in $G/N$, similar to what we did when proving Wilson's Theorem 3.1. We find

$$\begin{aligned} \pi = \prod_{g\in G/N} g &= \prod_{a=1}^{(p-1)/2} \prod_{b=1}^{q-1} (a,b)N \\ &= \prod_{a=1}^{(p-1)/2} \big(a^{q-1},\ (q-1)!\big)N \\ &= \Big(\big(\tfrac{p-1}{2}\big)!^{q-1},\ (q-1)!^{(p-1)/2}\Big)N \end{aligned}$$

Now by Wilson's Theorem 3.1, $(q-1)! \equiv -1 \pmod q$. By its Corollary 3.2, we also know that $\big(\frac{p-1}{2}\big)!^2 \equiv -(-1)^{(p-1)/2} \pmod p$ and raising this to the power $(q-1)/2$, we get

$$\begin{aligned} \pi &= \Big(\big(-(-1)^{(p-1)/2}\big)^{(q-1)/2},\ (-1)^{(p-1)/2}\Big)N \\ &= \Big((-1)^{(q-1)/2}\cdot(-1)^{(p-1)/2\cdot(q-1)/2},\ (-1)^{(p-1)/2}\Big)N \end{aligned} \tag{4}$$

Not that it matters for the proof, but one can check that

$$\pi = \begin{cases} (1,1)N = N & \text{if } p \equiv q \equiv 1 \pmod 4 \\ (1,-1)N = \big\{(1,-1),(-1,1)\big\} & \text{else.} \end{cases}$$

Now we use the Chinese remainder Theorem. Recall from the proof of Theorem 2.1, that there is a group isomorphism

$$\begin{aligned} \Psi\colon \big(\mathbb{Z}/pq\mathbb{Z}\big)^* &\to \big(\mathbb{Z}/p\mathbb{Z}\big)^* \times \big(\mathbb{Z}/q\mathbb{Z}\big)^* \\ c + pq\mathbb{Z} &\mapsto \big(c+p\mathbb{Z}, c+q\mathbb{Z}\big) \end{aligned}$$

Write $G'$ for the group $\big(\mathbb{Z}/pq\mathbb{Z}\big)^*$. Under $\Psi$, the subgroup $N$ corresponds to the subgroup $N' \leqslant G'$ given by $N' = \big\{1 + pq\mathbb{Z}, -1 + pq\mathbb{Z}\big\}$. Now each coset in $G'/N'$ is a pair $\big\{c + pq\mathbb{Z}, -c + pq\mathbb{Z}\big\}$. So if we run over all $1 \leqslant c \leqslant \frac{pq-1}{2}$ which are coprime to $p$ and $q$, then $(c + pq\mathbb{Z})N'$ will run through all cosets in $G'/N'$. Applying $\Psi$ to this, we see that

$$G/N = \Big\{(c,c)N \;\Big|\; 1 \leqslant c \leqslant \tfrac{pq-1}{2} \text{ and } (c,pq) = 1\Big\}.$$

**Example.** Let us make this explicit for the case $p = 5$ and $q = 7$ again. The group $G/N$ can also be presented as

$$\begin{gathered}(1,1)N \quad (2,2)N \quad (3,3)N \quad (4,4)N \quad (6,6)N = (1,6)N \quad (8,8) = (3,1)N \\ (9,9) = (4,2)N \quad (11,11)N = (1,4)N \quad (12,12)N = (2,5)N \\ (13,13)N = (3,6)N \quad (16,16)N = (1,2)N \quad (17,17)N = (2,3)N\end{gathered}$$

$\diamond$

Now in this new presentation, we can also compute the product of all elements in $G/N$.

$$\pi = \prod_{\substack{1 \leqslant c \leqslant \frac{pq-1}{2} \\ (c,pq)=1}} (c,c)N$$

Let's look at the first component alone. We group the factors from 1 to $p-1$, then from $p+1$ to $2p-1$ etc. Note the product runs up to $\frac{pq-1}{2} = \frac{q-1}{2}p + \frac{p-1}{2}$. In the end we have to divide by those factors which are not coprime to $q$, i.e. by $q$, $2q$, ...

$$\prod_{\substack{1 \leqslant c \leqslant \frac{pq-1}{2} \\ (c,pq)=1}} c = \frac{1}{1 \cdot q \cdot 2q \cdot \ldots \cdot \frac{p-1}{2} q} \cdot \prod_{c=1}^{p-1} c \cdot \prod_{c=p+1}^{2p-1} c \cdots \prod_{c=(\frac{q-1}{2}-1)p+1}^{\frac{q-1}{2}p-1} c \cdot \prod_{c=\frac{q-1}{2}p+1}^{\frac{pq-1}{2}} c$$

Note that all the $\prod$ in the above right hand side, except the very last one, are just $(p-1)!$ modulo $p$. The last product is $(\frac{p-1}{2})!$ instead. So this simplifies to

$$\begin{aligned}\prod_{\substack{1 \leqslant c \leqslant \frac{pq-1}{2} \\ (c,pq)=1}} c &\equiv \frac{(p-1)!^{(q-1)/2} \cdot \big(\frac{p-1}{2}\big)!}{q^{(p-1)/2} \cdot \big(\frac{p-1}{2}\big)!} \pmod p \\ &\equiv \frac{(-1)^{(q-1)/2}}{\left(\frac{q}{p}\right)} \equiv (-1)^{(q-1)/2} \cdot \left(\frac{q}{p}\right) \pmod p,\end{aligned}$$

where we used Euler's criterion in Proposition 4.2 and the fact that $(\frac{p}{q})$ is $\pm 1$.

The computation on the second component is similar and we find

$$\pi = \Big((-1)^{(q-1)/2} \cdot (\tfrac{q}{p}),\ (-1)^{(p-1)/2} \cdot (\tfrac{p}{q})\Big)N \tag{5}$$

Now we can compare the equation (4) and (5). It is clear that both are either $N$ or $(1,-1)N$. We can detect in which of the two $(a,b)N$ is by just looking at $ab \in \pm 1$. Here we get that

$$(-1)^{(q-1)/2} \cdot (-1)^{(p-1)/2 \cdot (q-1)/2} \cdot (-1)^{(p-1)/2} = (-1)^{(q-1)/2} \cdot (\tfrac{q}{p}) \cdot (-1)^{(p-1)/2} \cdot (\tfrac{p}{q})$$

This simplifies to $(\frac{p}{q}) \cdot (\frac{q}{p}) = (-1)^{(p-1)/2 \cdot (q-1)/2}$, which is what we wanted to prove.

# 5 Diophantine equations

An equation (usually polynomial) is called a *diophantine equation* if we are interested in its solutions in the set of integers or rational numbers.

**Example.** The equation $2x + 3y = 1$ has an integer solution $(x, y) = (-1, 1)$. The equation $x^2 = 2$ has no rational solution and by the same argument $x^2 = 2y^2$ has no integer solution. ◇

## 5.1 Linear diophantine equations

Given integers $a$, $b$, and $c$, we consider the equation

$$a\,x + b\,y = c \tag{6}$$

in two unknowns $x$ and $y$. We will assume $a \neq 0$ and $b \neq 0$. The solutions with $x, y$ in $\mathbb{Q}$ or $\mathbb{C}$ are easy; here we are looking for $x, y \in \mathbb{Z}$.

**Theorem 5.1.** *Set $d = (a, b)$. If $d \nmid c$, then the equation (6) has no integer solutions. If $d \mid c$, then there are infinitely many integer solutions. If $\xi$ and $\eta$ are such that $a\xi + b\eta = d$, then all solutions are given by*

$$x = \frac{c}{d}\,\xi + \frac{b}{d} \cdot k, \qquad \text{and} \qquad y = \frac{c}{d}\,\eta - \frac{a}{d} \cdot k,$$

*where $k$ ranges over the set of integers.*

*Proof.* Finding all $x \in \mathbb{Z}$ such that there is a $y \in \mathbb{Z}$ satisfying (6) is equivalent to finding $x \in \mathbb{Z}$ such that $a\,x \equiv c \pmod{b}$. So we can apply Theorem 1.2. If $d \nmid c$, then there are no solutions.

Assume now that $d \mid c$. The solutions to $a\,x \equiv c \pmod{b}$ form a unique congruence class modulo $b' = b/d$. Since $x_0 = c/d \cdot \xi$ and $y_0 = c/d \cdot \eta$ is a solution to (6), the solutions to the congruence equation form the congruence class $x_0 + b'\mathbb{Z}$. Now if $x = x_0 + kb'$ for some integer $k$, then we get

$$\begin{aligned} c &= a\,(x_0 + k\,b') + b\,y \\ &= a\,\big(\frac{c}{d}\xi + k\frac{b}{d}\big) + b\,y \\ &= \frac{c}{d}\,(d - b\eta) + a\,k\frac{b}{d} + b\,y. \end{aligned}$$

This implies that

$$0 = b\,\big(y - \frac{c}{d}\eta + k\frac{a}{d}\big)$$

and since $b \neq 0$, we get the expression for $y$ in the theorem. □

## 5.2 Non-linear diophantine equations

Let $f(x, y, z, \dots)$ be a polynomial with integer coefficients. If we started with a polynomial with rational coefficients, we could multiply it with the common denominator to achieve integer coefficients.

The question of finding rational solution reduced to the question of finding integer solutions: Write the unknown as $x = X/d$, $y = Y/d$, ... where $X$, $Y$, ..., $d$ are integers. Then multiply $f(\frac{X}{d}, \frac{Y}{d}, \dots)$ by a sufficiently high power of $d$. Now we have a new polynomial equation in one more variable for which we look for integer solutions.

On the one hand, there are two easy ways to prove that an equation does not have an integer solution: Inequalities and congruences. The two lemma below are obvious, yet useful.

**Lemma 5.2.** *Let $f(x, y, z, \dots)$ be a polynomial with integer coefficients such that $f(x, y, z, \dots) > 0$ for all real $x, y, z, \dots$. Then $f(x, y, z, \dots) = 0$ has no integer solution.*

**Example.** The equation $x^4 + 17\,x^2\,y^6 + 9\,z^2 + 19 = 0$ has no solution because the right hand side is always larger or equal to 19. ◇

**Lemma 5.3.** *Let $f(x, y, z, \dots)$ be a polynomial with integer coefficients such that $f(x, y, z, \dots) \equiv 0 \pmod m$ has no solution for some $m > 1$. Then $f(x, y, z, \dots) = 0$ has no integer solution.*

**Example.** The equation $x^3 - y^3 = 3$ does not have a solution modulo 9, so it can not have an integer solution. Inequalities would not help here as there are plenty of real solutions to it. ◇

On the other hand if we suspect an integer solution, it is often very difficult to find one. For instance $x^4 + y^4 + z^4 = t^4$ has plenty of solutions with non-zero $x$, $y$ and $z$. Yet, the smallest solution is

$$95800^4 + 217519^4 + 414560^4 = 422481^4.$$

(It was a conjecture of Euler that there were none, disproved by Elkies in 1987.)

If the equation has only finitely many solutions in $\mathbb{C}$, then we can just compute them to very high precision and check if any integer close-by is a solution. That is a way to solve equations $f(x) = 0$ in one variable; though that is not the best way to do so. If there are infinitely many solutions in the real numbers, then this method can not be used.

Let $f(x, y, z, \dots) = 0$ be a polynomial equation with coefficients in $\mathbb{Z}$. (It could even be a system of such equations.) Suppose it has infinitely many solutions in the real numbers. Suppose also that for each $m > 1$, there is a solution to this equation modulo $m$. Now both above methods fail to show that there are no solutions in integers. We would start by looking for integer solutions, by searching through all small $x$ and $y$. Even if we know that there are no solutions with $|x| < 10^6$, we would have no guarantee that there are no solutions in general. These are the really difficult diophantine equations.

**Aside:** *Modulo all $m$?* It looks like an infinite amount of work to check that an equation has a solution modulo $m$ for all $m$. We saw that the problem is essentially equivalent to finding solutions modulo $p$ for all primes $p$ using Hensel's lemma and the Chinese remainder theorem.

Now if there are infinitely many solutions to the equation over $\mathbb{R}$, then there is a constant $C$ such that the equation has automatically a (liftable) solution modulo $p$ for all primes $p > C$. Given the equation, one can, in principle, determine $C$ effectively. For instance for an equation like $ax^3 + by^3 + cz^3 = 0$ with pair-wise coprime non-zero integer constants $a$, $b$, $c$, then $C$ can be taken to be the largest prime divisor of $3abc$. The general result is a consequence of the work of many mathematicians starting with André Weil in the 1940s and culminating with the work of Pierre Deligne that won him the Fields medal in 1978. ◇

There is some good news. Consider an equation $f(x, y, z, \dots) = 0$ of total degree 2, like for instance

$$3\,x^2 + 10\,xy + 4\,y^2 + 12\,x - 6\,y - 21 = 0.$$

They are called quadratic forms. Minkowski proved that such a quadratic form has a rational solution if and only if it has a real solution and a solution modulo $m$ for all $m > 1$. The proof involves a method called the "geometry of numbers". A good exposition of Minkowski's theorem can be found in Serre's "Course in arithmetic" QA155 SER.

However, there is some bad news. This only holds for quadratic forms. For instance Selmer found that $3x^3 + 4y^3 + 5z^3 = 0$ has no non-trivial solution, yet it has plenty of real solutions and also a non-trivial solution modulo $m$ for all $m > 1$. Here is another example of this.

**Theorem 5.4** (Lind 1940, Reichardt 1942)**.** *There are no rational numbers $x$ and $y$ such that $2y^2 = 1 - 17x^4$.*

It is easy to show that there are real solutions: A picture of the curve can be seen in Figure 4 at the end of the notes. The corresponding equation for integers (see (7) below) has a non-trivial solution modulo

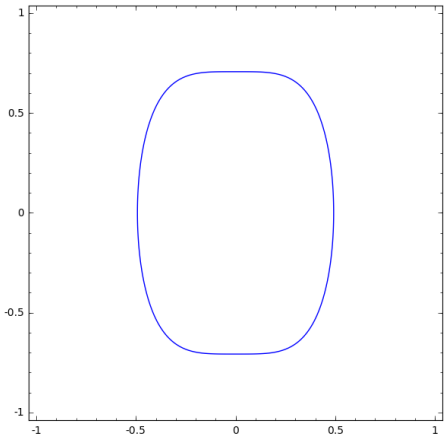



Figure 4: The real solutions to the equation of Lind and Reichardt in Theorem 5.4

all integers $m > 1$. Hence the proof has to use something stronger; in our case it is going to be the quadratic reciprocity law.

*Proof.* Suppose $(x, y)$ is a solution. Write $x = X/Z$ as a reduced fraction. Then

$$2y^2 = \frac{Z^4 - 17X^4}{Z^4}$$

shows that the denominator of $y$ must be $Z^2$ as the right hand side is again a reduced fraction. So we may write $y = Y/Z^2$ for some integer $Y$ which is coprime to $Z$. We obtain the new equation

$$2Y^2 = Z^4 - 17\,X^4 \tag{7}$$

to be solved in integers $X$, $Y$, $Z$ with $(X, Z) = 1$ and $(Y, Z) = 1$.

Note first that 17 can not divide $Y$: If it did, then $Z$ would also be divisible by 17, but that is not allowed as $(Y, Z) = 1$. Now let $p$ be a prime factor of $Y$. Hence $p \neq 17$. If $p = 2$, then $(\frac{p}{17}) = +1$ as $17 \equiv 1 \pmod 8$. If $p \neq 2$, then from the equation $Z^4 \equiv 17X^4 \pmod p$, we see that 17 must be a quadratic residue modulo $p$. Hence $(\frac{17}{p}) = +1$. By the quadratic reciprocity law (Theorem 4.6), this implies that $(\frac{p}{17}) = +1$ because $17 \equiv 1 \pmod 4$.

Therefore we have shown that all prime factors of $Y$ are quadratic residues modulo 17, which shows that $Y$ is a quadratic residue modulo 17. From $2Y^2 \equiv Z^4 \pmod{17}$ we now deduce that 2 should be a $4^{\text{th}}$ power modulo 17. However only 1, 4, $-4$ and $-1$ are fourth powers modulo 17 which means that we have reached a contradiction. □