1 Prime Numbers and Arithmetic

Definition. A **prime number** is a positive integer p who has exactly two positive divisors, namely 1 and p.

Notation. For $m, n \in \mathbb{Z}$ write $m \mid n$ to mean m divides n, i.e. $n = am$ for some $a \in \mathbb{Z}$.

Definition. Let p be a prime number. Given an integer $n \neq 0$, we write $\operatorname{ord}_p(n)$ for the largest power of p dividing n. So $p^{\operatorname{ord}_p(n)}$ divides n, but $p^{\operatorname{ord}_p(n)+1}$ does not.

Fundamental theorem of Arithmetic 1.1. *Every nonzero $n \in \mathbb{Z}$ has a factorisation*

$$n = \operatorname{sign}(n) \cdot \prod_{\text{primes } p} p^{\operatorname{ord}_p(n)} \qquad \textit{where} \qquad \operatorname{sign}(n) = \begin{cases} +1 & \textit{if } n > 0, \\ -1 & \textit{if } n < 0. \end{cases}$$

This factorisation is unique. Each n has only a finite number of prime divisors, so the product is really finite: for each n, the exponent $\operatorname{ord}_p(n) = 0$ for all but a finite number of primes p.

Definition. The **greatest common divisor** of $m, n \in \mathbb{Z}$ is the largest integer which divides both m and n. Notation: $\gcd(m, n)$.

Euclidean algorithm can be used to find $g = \gcd(m, n)$ and also integers x, y such that $g = mx + ny$.

Notation. For $m \geqslant 1$ write $a \equiv b \pmod{m}$, read as "a is **congruent** to b modulo m", to mean $m \mid (a - b)$.

Chinese Remainder Theorem 1.2. *Let m_1, m_2, $\dots m_r$ be pairwise coprime integers and let a_1, a_2, $\dots a_r$ be integers. Then solving the congruences $x \equiv a_i \pmod{m_i}$ for all $1 \leqslant i \leqslant r$ is equivalent to solving a congruence $x \equiv b \pmod{m_1 \cdot m_2 \cdots m_r}$ for some integer b.*

Theorem 1.3. *There are infinitely many primes.*

Proof. Suppose that there are only finitely many primes, say p_1, p_2, $\dots$, p_k. Then $n = 1 + \prod_{i=1}^{k} p_i$ must have a prime factor not in $\{p_1, \dots, p_k\}$. □

Definition. An integer a is **square-free** if it has no square divisors greater than 1; alternatively, if $\operatorname{ord}_p(a) \in \{0, 1\}$ for all primes p.

Lemma 1.4. *If $n \in \mathbb{Z}$ is nonzero then $n = a \cdot b^2$ with a square-free.*

Proof. Take b^2 to be the largest divisor of $|n|$ which is a square and set $a = n/b^2$. If a square c^2 divides a, then $c^2 b^2$ divides n. So by the maximality of b, we have $c = 1$ and a is square-free. □

Arithmetic Functions and the Möbius inversion theorem

Definition. An **arithmetic function** is any function $f \colon \mathbb{N} \to \mathbb{C}$.

Examples. Functions that you have seen in G12ALN like $\tau(n)$, counting the number of divisors of n, or $\sigma(n)$, the sum of all divisors of n. More generally we set $\sigma_k(n) = \sum_{d \mid n} d^k$, so that $\tau = \sigma_0$ and $\sigma = \sigma_1$. And there is Euler's totient function $\varphi(n)$ counting the number of integers $1 \leqslant m \leqslant n$ that are coprime to n.

n	1	2	3	4	5	6	7	8	9	10	11	12	...	p prime
$\tau(n)$	1	2	2	3	2	4	2	4	3	4	2	6		2
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18	12	28		$p+1$
$\sigma_2(n)$	1	5	10	21	26	50	50	85	91	130	122	210		p^2+1
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4		$p-1$

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

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

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 1.5. *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 $f * g$, defined by

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

The arithmetic functions I and ε are defined by $I(n) = 1$ for all n and

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

Properties of convolution 1.6. *For all 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 symetry of the formula $(f * g)(n) = \sum_{ed=n} f(e)g(d)$. The second 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 symetric again so it equals $\Big((f * g) * h\Big)(n)$ for all n. Propertiy iv) is easy for $n = 1$ and is exactly what the previous lemma says for $n > 1$. The last property is easy again. □

Möbius Inversion Theorem 1.7. *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

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

Theorem 1.8. *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. For $n = 1$, we have $g(1) = (f * g)(1) = \varepsilon(1) = 1$. Let $n > 1$. By induction, assume that $g(k)$ was constructed for all $k < n$. Then $(f * g)(n) = \varepsilon(n) = 0$ gives

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

Corollary 1.9. *Let f and h be arithmetic functions such that $f(1) = h(1) = 1$. Then there exists a unique arithmetic function g such that $f * g = h$.*

Proof. Take $g = g_1 * h$ where $f * g_1 = \varepsilon$. □

Example. The Dirichlet inverse of I is μ, of course. What is Dirichlet inverse of τ ? We are looking for a function g such that $\tau * g = \varepsilon$. We can write $\tau = I * I$ and solve the equation on g:

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

Primitive elements

Recall that the Euler function $\varphi(m)$ counts the number of integer in $1 \leqslant a \leqslant m$ that are coprime to m.

Theorem 1.10. *Let $m > 1$. For all a coprime to m, we have $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

The proof was given in G12ALN 5.4.6. In the problem sheet we will prove that $\varphi = \mu * \mathrm{id}$ where $\mathrm{id}(n) = n$.

Definition. Let $m > 1$ be an integer and a an integer coprime to m. The **multiplicative order** $r(a)$ of a modulo m is the smallest integer $k > 0$ such that $a^k \equiv 1 \pmod{m}$.

The multiplicative order of elements modulo 13 are listed in the following table.

a	1	2	3	4	5	6	7	8	9	10	11	12
$r(a)$	1	12	3	6	4	12	12	4	3	6	12	2

Lemma 1.11. *The multiplicative order $r(a)$ divides $\varphi(m)$ for all $\gcd(a, m) = 1$.*

Proof. Let $k = \gcd\bigl(r(a), \varphi(m)\bigr)$. There are integers x and y such that $k = x\, r(a) + y\, \varphi(m)$. So

$$a^k = a^{x\, r(a) + y\, \varphi(m)} = \bigl(a^{r(a)}\bigr)^x \cdot \bigl(a^{\varphi(m)}\bigr)^y \equiv 1^x \cdot 1^y = 1 \pmod{m}$$

and the minimality of $r(a)$ imply that $k = r(a)$. □

Definition. An integer g is called a **primitive element** modulo m if it has multiplicative order equal to $\varphi(m)$.

Sometimes they are also called **primitive root** modulo m.
Primitive elements do not exist for all integers m, for instance for $m = 12$ and $m = 15$ there are no primitive elements:

a	1	5	7	11
$r(a)$	1	2	2	2

Multiplicative order modulo 12

a	1	2	4	7	8	11	13	14
$r(a)$	1	4	2	4	4	2	4	2

Multiplicative order modulo 15

Theorem 1.12. *Let p be a prime. Then there exist a primitive element g modulo p.*

Proof. By Fermat's Little Theorem $a^{p-1} \equiv 1 \pmod{p}$ for $p \nmid a$, so $X - a$ divides $X^{p-1} - 1$ in ${}^{\mathbb{Z}}/_{p\mathbb{Z}}[X]$. Hence

$$X^{p-1} - 1 = (X-1)(X-2)(X-3)\cdots(X-(p-1))$$

Let $d \mid (p-1)$. The solutions a of $X^d - 1$ are exactly the elements with $r(a)$ dividing d. Writing $p - 1 = dm$, we get

$$\bigl(X^d - 1\bigr)\bigl(1 + X^d + X^{2d} + \cdots + X^{(m-1)d}\bigr) = X^{p-1} - 1.$$

So $X^d - 1$ also factors into linear factors and there are d solutions to it.
Let $\psi(d)$ be the number of elements $1 \leqslant a < p$ with multiplicative order d. We have shown that $d = \sum_{c|d} \psi(c)$. In other words $\mathrm{id} = \psi * I$. Hence $\psi = \mathrm{id} * \mu = \varphi$. So there are exactly $\varphi(p-1) > 0$ elements of multiplicative order $p - 1$ modulo p. □

Corollary 1.13. *Let p be a prime and let a be an integer coprime to p. Given a primitive element g there exists exactly one $0 \leqslant k < p - 1$ such that $a \equiv g^k \pmod{p}$.*

Proof. The list $\{g^0, g^1, g^2, \ldots, g^{p-2}\}$ does not contain two elements that are congruent modulo p; otherwise $g^i \equiv g^j \pmod{p}$ and so g would have order $|j - i| < p - 1$. Since there are $p - 1$ elements, every non-zero residue class modulo p must appear exactly once in this list. □

Note though, that there is no obvious choice for a primitive element. Often a small integer like 2, 3, 5, or 6 will be a primitive element. There are important open question on primitive elements like Artin's conjecture which asks if any integer $a > 1$ is a primitive element for infinitely many primes p, unless a is a square. In fact, it should happen roughly for 37.396% of all primes p.
Primitive elements are also crucial for cryptography, like Elgamal's cipher (see G13CCR).