Number Theory

October 16, 2019

1 Euclid's Algorithm

Theorem 1.1 (Division Algorithm)**.** *Given $a, b \in \mathbb{Z}, b > 0$, we can determine $\exists q, r \in \mathbb{Z}$ s.t. $a = qb + r$ with $0 \leq r < b$.*

Proof. Let $S = \{a - nb : n \in \mathbb{Z}\}$. S contains some non-negative integer. Let r be the least such integer, say $a - qb$. Then $a = qb + r$, so STP $r < b$.

Suppose $b \leq r$. Then $0 < r - b = a - (q+1)b \in S$, and $r - b < r$. $\lightning$ (choice of r) $\square$

If $r = 0$, i.e. if $a = qb$ for some $q \in \mathbb{Z}$, then we write $b|a$ and say "b ***divides*** a" or "b is a ***divisor*** of a". If $r \neq 0$, then we instead write $b \nmid a$ and say "b does ***not divide*** a".

Given $a_1, \ldots, a_n \in \mathbb{Z}$ not all 0, let $I = \{\lambda_1 a_1 + \ldots + \lambda_n a_n : \lambda_i \in \mathbb{Z}\}$. Observe if $a, b \in I, \ell, m \in \mathbb{Z}$, then $\ell a + mb \in I$.

Theorem 1.2. *$I = d\mathbb{Z} = \{dm : m \in \mathbb{Z}\}$ for some $d > 0$*

Proof. I contains some positive integer. Let $d > 0$ be the least such. Then clearly $I \supseteq d\mathbb{Z}$.

Conversely, let $a \in I$ and apply **1.1** to obtain $a = qd + r$ for some $q, r \in \mathbb{Z}$, $0 \leq r < d$. Then $r = a - qd \in I \implies r = 0$, so $d\mathbb{Z} \supseteq I$

$\therefore I = d\mathbb{Z}$ $\square$

Note that $a_i \in I \forall i$, so $d | a_i \forall i$. Conversely, if $c | a_i \forall i$ then c divides every element of I, so in particular $c|d$.

We write $d = \gcd(a_1, \ldots, a_n) = (a_1, \ldots, a_n)$, and say d is the ***greatest common divisor*** of the a_i.

Corollary 1.3 (Bézout)**.** *Let $a, b \in \mathbb{Z}$, a, b not both 0. Then $\exists x, y \in \mathbb{Z}$ s.t. $ax + by = c \iff (a, b) | c$.*

The division algorithm gives an efficient method for computing (a, b).

Theorem 1.4 (Euclid's Algorithm)**.** *Suppose $a > b > 0$. Then:*

$$\begin{aligned} a &= q_1 b + r_1 & 0 \le r_1 < b \\ b &= q_2 r_1 + r_2 & 0 \le r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 & 0 \le r_3 < r_2 \\ &\vdots \\ r_{k-2} &= q_k r_{k-1} + r_k & r_k \neq 0 \\ r_{k-1} &= q_{k+1} r_k (+0) \end{aligned}$$

and $r_k = (a, b)$

Proof. We have $r_k | r_{k-1} \implies \dots \implies r_k | a, r_k | b \implies r_k | (a, b)$, so $r_k \le (a, b)$. Note also that any m s.t. $m|a$ and $m|b$ also divides r_k. In particular, $(a, b) | r_k$, and thus $(a, b) \le r_k$, hence $r_k = (a, b)$. $\square$

Additionally, by working back up the algorithm, we can obtain a representation $(a, b) = \lambda a + \mu b$ where $\lambda, \mu \in \mathbb{Z}$

An integer $n > 1$ is ***prime*** if its only positive divisors are 1 and n. Otherwise, we say n is ***composite***.

Lemma 1.5. *Let p be a prime, $a, b \in \mathbb{Z}$. Then $p | ab \iff p | a$ or $p | b$*

Proof. It is clear that if $p|a$ or $p|b$, then $p|ab$. Conversely, suppose $p|ab$ but $p \nmid a$. Them $(a, p) \neq p$. By definition, $(a, p) | p \implies (a, p) \in \{1, p\}$, so $(a, p) = 1$. Now by **1.3** we can find $x, y \in \mathbb{Z}$ s.t. $1 = ax + by \implies b = b(ax + py) = x(ab) + (by)p$, so $p|b$. $\square$

Theorem 1.6 (The Fundamental Theorem of Arithmetic)**.** *Every integer $n > 1$ can be written as a product of primes uniquely up to reordering*

Proof. We have existence by strong induction.

For uniqueness, n is the least integer with two distinct such representations, say $= n = p_1 \dots p_s = q_1 \dots q_r$ for p_i, q_j primes.
Then $p_1 | q_1 \dots q_r \implies p_1 | q_j$ for some j. WLOG $j = 1$. Since $p_1 > 1$ as 1 is non-primes, $n/p_1 < n$, and $n/p_1 = p_2 \dots p_s = q_2 \dots q_r$ can be written in two distinct ways as a product of primes. $\lightning$ (choice of n) $\square$

If $m = \Pi_{i=1}^k p_i^{\alpha_i}, n = \Pi_{i=1}^k p_i^{\beta_i}$ where p_i are distinct primes, $\alpha_i, \beta_i \ge 0$, then $(m, n) = \Pi_{i=1}^k p_i^{\gamma_i}$ with $\gamma_i = \min\{\alpha_i, \beta_i\}$. However, if m, n are large, it is much more "efficient" to compute the gcd via Euclid's algorithm.

An algorithm with input $N > 0$ is said to run in ***polynomial time*** if it takes at most $c(\log N)^k$ elementary operations to complete, where $c, k > 0$ are constants independent of N. If the algorithm takes inputs $N_1, N_2, \dots, N_s$, the polynomial time means $c(\max \log N_i)^k$.

Examples of polynomial time algorithms:

- Adding and multiplying integers
- The gcd of two numbers via Euclid's algorithm

- Testing of primality

On the other hand, factoring a number into prime factors does not have a polynomial time algorithm, and it is conjectured that one does not exist. For instance, if $N = p \cdot q$ with p, q primes of ~ 50 digits each, to do trial division up to $\sqrt{N}$ at a rate of 2^9 divisions per second, it would take approximately $\sqrt{10^{100}}/2^9$ seconds, or about 6×10^39 years. However, we can compute the gcd in milliseconds using Euclid's algorithm.

Theorem 1.7. *There are infinitely many primes. i.e.* $\pi(x) \to \infty$ *as* $x \to \infty$

Proof. Fix $N > 1$, let p be the largest prime $\leq N$. Let q be a prime factor of $M = (2 \times 3 \times 5 \times \ldots \times p) + 1$. Then $q > N$ since $q \notin \{2, 3, \ldots, p\}$, but N was arbitrary. □

2 Congruences

Let $n \geq 1$ be an integer. We write $a \equiv b \mod n$ if $n | a - b$. This defines an equivalence relation on $\mathbb{Z}$, and we will write $\mathbb{Z}/n\mathbb{Z}$ for the equivalence classes induced by this relation, which are $a + n\mathbb{Z}$ for $0 \leq a < n$. It is easy to check that $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b + n\mathbb{Z})$ and that $(a + n\mathbb{Z}) \times (b + n\mathbb{Z}) = (ab + n\mathbb{Z})$ are well defined operations, i.e $n\mathbb{Z}$ is an ideal, and $\mathbb{Z}/n\mathbb{Z}$ is the quotient ring.

Lemma 2.1. *Let* $a \in \mathbb{Z}$. *Then the following are equivalent:*

1. $(a, n) = 1$
2. $\exists b \in \mathbb{Z}$ *s.t.* $ab \equiv b \mod n$
3. *The equivalence class of* a *generates the group* $(\mathbb{Z}/n\mathbb{Z}, +)$

Proof.

- (1) $\implies$ (2): $(a, n) = 1 \implies \exists b, c \in \mathbb{Z}$ s.t. $ab + cn = 1$ by **1.3**, and hence $ab \equiv 1 \mod n$.
- (2) $\implies$ (1): $ab \equiv 1 \mod n \iff ab - 1 = kn$ for some $k \in \mathbb{Z}$, and so by **1.3** $(a, n) = 1$.
- (2) $\iff$ (3): $ab \equiv 1 \mod n \iff 1 \in \langle a \rangle \leq \mathbb{Z}/n\mathbb{Z} \iff \langle a \rangle = \mathbb{Z}/n\mathbb{Z}$

□

We write $(\mathbb{Z}/n\mathbb{Z})^\times$ for the set of ***units*** (the elements with a multiplicative inverse) of $\mathbb{Z}/n\mathbb{Z}$. By **2.1**, $(\mathbb{Z}/n\mathbb{Z})^\times$ contains precisely those classes $a + n\mathbb{Z}$ such that $(a, n) = 1$. Note that if $n > 1$ then $\mathbb{Z}/n\mathbb{Z}$ is a field precisely when n is prime.

Let ***Euler's*** φ ***function*** be $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$ for $n > 1$, and let $\varphi(1) = 1$. Observe that $\varphi(p) = p - 1$ for p prime. Moreover, φ is a multiplicative function: $(m, n) = 1 \implies \varphi(mn) = \varphi(m)\varphi(n)$.

Corollary 2.2. *Let* G *be a cyclic group of order* $n \geq 1$. *Then* $\varphi(n) = |\{g \in G : \mathrm{ord}(g) = n\}|$, *the number of generators of* G.

Theorem 2.3 (Euler-Fermat)**.** *IF* $(a, n) = 1$, $a, n \in \mathbb{Z}$, *then* $a^{\varphi(n)} \equiv 1 \mod n$

Proof. By Lagrange's Theorem, the order of a in the group $(\mathbb{Z}/n\mathbb{Z})^\times$ divides the order of $(\mathbb{Z}/n\mathbb{Z})^\times$, which is $\varphi(n)$ □

Theorem 2.4 (Fermat's Little Theorem)**.** *If $a, p \in \mathbb{Z}$ and p is prime, then $a^p \equiv a \mod p$.*

Proof. If $p|a$, then this holds trivially. If $p \nmid a$, $(a,p) = 1$ and so by **2.3** we have $a^{\varphi(p)} \equiv a^{p-1} \equiv 1 \mod p$ $\square$

Multiple Congruences

Can we find all $x \in \mathbb{Z}$ s.t. $x \equiv 4 \mod 7$ and $x \equiv 5 \mod 12$?

Suppose we can find $u, v \in \mathbb{Z}$ s.t. $\begin{cases} u \equiv 1 \mod 7; & u \equiv 0 \mod 12 \\ v \equiv 0 \mod 7; & v \equiv 1 \mod 12 \end{cases}$. Then we can write down that $x = 4u + 5v$. Since $(7, 12) = 1$, by **1.3** there are some $m, n \in \mathbb{Z}$ with $7m + 12n = 1$, and from Euclid's algorithm we can determine these to be $m = -5, n = 3$. Then we can find $u = 12n = 1 - 7m; v = 7m = 1 - 12n$, and substitution gives $u = 36, v = -35$, and so a solution to the original problem is $4 \times 36 - 5 \times 35 = -31$. Now the lowest common multiple of 7 and 12 is 84, and so our solution set is: $\{x \in \mathbb{Z} : x \equiv -31 \mod 84\}$.

We can in fact generalise this process:

Theorem 2.5 (Chinese Remainder Theorem)**.** *Let $m_1, \ldots, m_k$ be pairwise coprime positive integers, and let $M = \Pi_{i=1}^k m_i$. Then given any integers $a_1, \ldots, a_k$ there is a solution x to the the system of congruences:*

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_k \mod m_k \end{aligned}$$

Moreover, this solution is unique modulo M.

Note that if x satisfies this system of equations, then so does $x + tM$ for any $t \in \mathbb{Z}$, and so the complete set of solutions is $x + M\mathbb{Z}$.

Proof.

Uniqueness: If x, y satisfy the system, then $m_i | x - y$ for all $i = 1, \ldots, k$. Since no prime divides any tow the m_i, $M | x - y$ and hence $x \equiv y \mod M$.

Existence: Write $M_i = \frac{M}{m_i} = \Pi_{j \neq i} m_j$ for each $i = 1, 2, \ldots, k$. Since $(m_i, m_j) = 1 \forall i \neq j$, $(m_i, M_i) = 1$ for all $i = 1, 2, \ldots, k$. Therefore, for each $i = 1, 2, \ldots, k$ we can find $b_i \in \mathbb{Z}$ such that $M_i b_i \equiv 1 \mod m_i$ and $M_i b_i \equiv 0 \mod m_j$ for $j \neq i$. Then $x = \sum_{i=1}^k a_i b_i M_i$ solves the system of congruences. $\square$

If $m_1, \ldots, m_k$ are pairwise coprime, and $M = \Pi m_i$, then map $\theta : \mathbb{Z}/M\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_k\mathbb{Z}$, taking $x \mod M \mapsto (x \mod m_1, \ldots, x \mod m_k)$ is an isomorphism of rings. To see this, note that if $m_i | M$ then $x \mod m_i$ is determined by $x \mod M$ which implies that θ is well-defined. It is a homomorphism by the properties of $+, \times$ in $\mathbb{Z}/n\mathbb{Z}$, and **2.5** implies that θ is a bijection. In particular, if $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ for distinct primes p_i, then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$.

Corollary 2.6. *If $m_1, \ldots, m_k$ are pairwise coprime and $M = \Pi_{i=1}^k m_i$ and $a_1, \ldots, a_k \in \mathbb{Z}$ are such that $(a_i, m_i) = 1$ for each $i = 1, 2, \ldots, k$, then there is a solution to the system of congruences in **2.5**, and any such solution is in fact coprime to M.*

Proof. **2.5** gives us a solution, say $x \in \mathbb{Z}$. Suppose $(x, M) > 1$. Then there is a prime p such that $p|x$ and $p|M$ simultaneously. p prime, so WLOG suppose that p divides m_1. Since $x \equiv a_1 \mod m_1$, we must have $p|a_1$, and so $p|(a_1, m_1)$ $\lightning$. $\square$

Corollary 2.7. *If $m_1, \ldots, m_k$ are pairwise coprime with $M = \Pi_{i=1}^k m_i$, then $\varphi(M) = \varphi(m_1) \cdot \ldots \cdot \varphi(m_k)$*

A ***multiplicative function*** is a function $f : \mathbb{N} \to \mathbb{C}$ such that, for all $m, n \in \mathbb{N}$ coprime, $f(mn) = f(m)f(n)$. A function $f : \mathbb{N} \to \mathbb{C}$ is said to be ***totally multiplicative*** if for all $m, n \in \mathbb{N}$, $f(m, n) = f(m)f(n)$.

Some multiplicative functions are:

- $\varphi(m)$
- $\tau(n) =$ the number of positive divisors of n
- $\sigma(n) =$ the sum of the positive divisors of n
- $\sigma_k(n) = \sum_{d|n} d^k$, so that $\sigma_0(n) = \tau(n), \sigma_1(n) = \sigma(n)$.

None of these are totally multiplicative however.

Lemma 2.8. *Let f be a multiplicative function. Then so is g, where $g(n) = \sum_{d|n} f(d)$.*

Proof. Let $m, n \in \mathbb{N}, (m, n) = 1$. Then the divisors of mn are precisely the integers of the form $d_1 d_2$ where $d_1|m, d_2|n$ and $(d_1, d_2) = 1$. This means that we can write down

$$\begin{aligned}
g(mn) &= \sum_{d|mn} f(d) \\
&= \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) \\
&= \sum_{d_1|m} \sum_{d_2|n} f(d_1) f(d_2) \\
&= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) \\
&= g(m)g(n)
\end{aligned}$$

$\square$

Then if we let $f(n) = n^k$ for some $k \in \mathbb{N}$. Then $g(n) = \sum_{d|n} d^k = \sigma_k(n)$. Later on, we shall see that we can recover f from g via Möbius inversion.

Theorem 2.9.

1. *If p is a prime and $m \in \mathbb{N}$ then $\varphi(p^m) = p^{m-1}(p-1) = p^m \left(1 - \frac{1}{p}\right)$*
2. *$\forall n \in \mathbb{N}, \varphi(n) = n \cdot \Pi_{p|n} \left(1 - \frac{1}{p}\right)$*
3. *$\sum_{d|n} \varphi(d) = n$*

Proof.

1.

$$\begin{aligned}\varphi(p^m) &= |\{1 \leq a \leq p^m : (a, p^m) = 1\}| \\ &= p^m - p^{m-1} \\ &= p^m \left(1 - \frac{1}{p}\right)\end{aligned}$$

2. Let $n = \Pi_{i=1}^k p_i^{\alpha_i}$ for p_i distinct primes, $\alpha_1 \geq 1$. Then:

$$\begin{aligned} varphi(n) &= \Pi_{i=1}^k \varphi(p_i^{\alpha_i}) \\ &= \Pi_{i=1}^k p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) \\ &= n \cdot \Pi_{p|n} \left(1 - \frac{1}{p}\right)\end{aligned}$$

3. φ is multiplicative and so is $n \mapsto n$, so it suffices to check that both sides agree when n is a prime power. Let p be a prime $m \in \mathbb{N}$. Then:

$$\begin{aligned}\sum_{d|p^m} \varphi(d) &= \varphi(1) + \varphi(p) + \ldots + \varphi(p^m) \\ &= 1 + (p-1) + (p^2 - p) + \ldots + (p^m - p^{m-1}) \\ &= p^m\end{aligned}$$

$\square$