Number theory

RMS Black Team

Euclidean algorithm, Bézout, unique factorization

A useful way of computing the greatest common divisors of integers is by using the following fact: $(a, b) = (a, a - b)$ for all $a, b \in \mathbb{Z}$. The proof that this terminates relies on the following fact: for all $a, b \in \mathbb{Z}$, there exist $q, r \in \mathbb{Z}$ s.t. $|r| \leq \frac{|b|}{2}$. Then, we can repeatedly use the fact that $(a, b) = (r, b)$ to quickly compute the gcd of two numbers. This process is called the Euclidean algorithm, and it is quite useful in the settings in which one can get it to work.

Lemma 1 (Bézout). *For two relatively prime a, b, there exist $x, y \in \mathbb{Z}$ s.t. $ax + by = 1$.*

Proof. Let $(a_1, \ldots, a_n)_0 = \{a_1x_1 + \cdots + a_nx_n : x_1, \ldots, x_n \in \mathbb{Z}\}$. Then, it is necessary and sufficient to show that $(a, b)_0 = \mathbb{Z}$. However, note that we have that $(a, b)_0 = (a, a - b)_0$. This is highly suggestive of the Euclidean algorithm, and in fact, by repeatedly applying this in the same way one would use the Euclidean algorithm to compute (a, b), one can show that $(a, b)_0 = (1)_0 = \mathbb{Z}$ as desired. $\square$

We shall now use this to prove the following very useful fact about primes

Lemma 2 (Euclid). *If p is prime, $p|ab$, then we have that either $p|a$ or $p|b$.*

Proof. If $p|a$, we are done, so suppose that $(a, p) = 1$. Otherwise, by Bézout, there exist $x, y \in \mathbb{Z}$ such that $px + ay = 1$. It follows that $pbx + aby = b$. However, note that $p|ab$, so it follows that $p|pbx + aby = b$, and the desired result follows. $\square$

With a bit of work, it is possible to use this to show the following:

Theorem 3 (Fundamental Theorem of Arithmetic). *For all nonzero n not equal to 1, there exist $p_1, \ldots, p_n$ that are unique up to permutation such that $n = \pm p_1 \ldots p_n$*

Proof. First, we shall show that n can be written as the product of primes, and then we shall show the uniqueness. Also, we shall suppose that n is positive for notational convenience.

We shall prove the first part by contradiction. Suppose, for the sake of contradiction, that n is the smallest positive integer that cannot be written as the product of primes. Then, clearly, n is not a prime, so there exist $a, b > 1$ s.t. $n = ab$. Then, clearly, $a, b < n$. However since n was assumed to be the smallest positive integer that could not be written as the product of primes, a, b must be expressible as the product of primes, which is a contradiction. The desired result follows.

For showing the uniqueness, suppose that there exist $p_1, \ldots, p_k$ and $\ell_1, \ldots, \ell_m$ that are distinct s.t. $n = p_1 \ldots p_k = \ell_1 \ldots \ell_m$. Also, take n minimal, so that we have that $\{p_1, \ldots, p_k\}$ and $\{\ell_1, \ldots, \ell_m\}$ are disjoint (otherwise, we could divide out the primes in common and get a smaller value that breaks unique factorization). However, we clearly have that $p_1|\ell_1 \ldots \ell_m$, so by Euclids lemma, there exists j s.t. $p_1|\ell_j$. However, ℓ_j is prime, so $p_1 = \ell_j$, which is a contradiction, as $\{p_1, \ldots, p_k\}$ and $\{\ell_1, \ldots, \ell_m\}$ are disjoint. The desired result follows. $\square$

The fact that unique factorization is true is not always true in settings other than $\mathbb{Z}$. For example, we have that in $\mathbb{Z}[\sqrt{-5}]$, $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \cdot 3$. We won't go over what exactly it means to be prime in $\mathbb{Z}[\sqrt{-5}]$, but just be aware that unique factorization is not very obvious.

Problems

1. Show that if $n|ab$, and $(a, b) = 1$, either $n|a$ or $n|b$.
2. Find x, y such that $124x + 263y = 1$.
3. (IMO) Show that $21x + 4$ and $14x + 3$ are relatively prime for all $x \in \mathbb{Z}$.

$\mathbb{Z}/(n)$, Chinese remainder theorem, Euler's theorem

We say that a is congruent to b modulo n or $a \equiv b \pmod{n}$ if $n|a-b$. It is not hard to show that if $a \equiv b \pmod{n}, c \equiv d \pmod{n}$, then $a+c \equiv b+d \pmod{n}, ac \equiv bd \pmod{n}$. For all n, we can split up the integers into n equivalence classes where two integers are in the same equivalence class if they are congruent modulo n (since congruence modulo n is an equivalence relation). This is written as $\mathbb{Z}/(n)$ or $\mathbb{Z}/n\mathbb{Z}$. Note that the parentheses around the n are actually important in this case. For example, $\mathbb{Z}/(3)$ consists of the elements $\{\dots, -3, 0, 3, \dots\}, \{\dots, -2, 1, 4, \dots\}, \{\dots, -1, 2, 5, \dots\}$. We can add elements of $\mathbb{Z}/(n)$ by taking the sum of every pair of elements in each of the two equivalence classes we are adding. Occasionally, we may do things like add elements of $\mathbb{Z}$ and $\mathbb{Z}/(n)$, which isn't technically correct as we should be adding the equivalence class of the element of $\mathbb{Z}$. However, it will typically will be clear what I mean.

Theorem 4 (Chinese remainder theorem)**.** *There is a bijection*

$$f : \mathbb{Z}/(n_1 \dots n_m) \to \mathbb{Z}/(n_1) \times \dots \times \mathbb{Z}/(n_m)$$

for pairwise relatively prime $n_1, \dots, n_m$. Also, we have that $f(a + b) = f(a) + f(b)$, and $f(ab) = f(a)f(b)$, where addition and multiplacation of elements in $\mathbb{Z}/(n_1) \times \dots \times \mathbb{Z}/(n_m)$ is done elementwise. (The Cartesian product $A \times B$ for two sets A, B is the set of ordered pairs (a, b) for $a \in A, b \in B$).

Equivalently, if $n \equiv k_i \pmod{n_i}$ for $1 \le i \le m$, then there exists some unique K modulo $n_1 \dots n_m$ s.t. $n \equiv K \pmod{n_1 \dots n_m}$.

Sketch of proof. We shall work with the second version, which clearly implies the first statement. It is sufficient to show that this holds for $m = 2$. To show the existence of solutions, one can use Bézout's lemma. For uniqueness, just note that if you know some integer modulo n for some n, then it is determined modulo all of its factors. $\square$

The use of the Chinese remainder theorem and related ideas is that one can often simply reduce a problem down to showing that some statement holds for prime powers.

From Bézout, it is also easy to see that the following holds:

Lemma 5 (Inverses modulo n)**.** *For all a relatively prime to n, there exists some $b \in \mathbb{Z}/(n)$ s.t. $ab \equiv 1 \pmod{n}$. This is called the inverse of a modulo n, and is often denoted a^{-1}.*

Now, let $(\mathbb{Z}/(n))^*$ be the set of invertible elements in $\mathbb{Z}/(n)$. Note that $(\mathbb{Z}/(n))^*$ is closed under multiplication. Also, we define the Euler totient function $\varphi(n)$ to be $|(\mathbb{Z}/(n))^*|$. By the Chinese remainder theorem, φ is multiplicative; we have that for relatively prime m, n, $\varphi(mn) = \varphi(m)\varphi(n)$. Therefore, if $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ for primes $p_1, \dots, p_k$, $\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \dots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})$.

Also, we have the following:

Theorem 6 (Euler's totient theorem)**.** *For all $(a, n) = 1$, we have $a^{\varphi(n)} \equiv 1 \pmod{n}$*

Proof. It is not hard to show that multiplication by some element $a \in (\mathbb{Z}/(n))^*$ simply permutes the elements of $(\mathbb{Z}/(n))^*$. Now, let

$$N = \prod_{k \in (\mathbb{Z}/(n))^*} k.$$

Then, we also have that

$$N = \prod_{k \in (\mathbb{Z}/(n))^*} ak = a^{\varphi(n)} N$$

for all $a \in (\mathbb{Z}/(n))^*$. It follows that since $N \in (\mathbb{Z}/(n))^*$, it is invertible, so we have that $a^{\varphi(n)} = 1$ in $(\mathbb{Z}/(n))^*$, as desired. $\square$

Corollary 1 (Fermat's little theorem)**.** *For all a, p s.t. $p \nmid a$, $a^{p-1} \equiv 1 \pmod{p}$.*

Problems

1. Find the smallest positive integer that is congruent to 1 (mod 2), 0 (mod 3), 2 (mod 5), and 10 (mod 13).
2. Find last 3 digits of $2^{2^{2^{2^{2^{2}}}}}$.
3. Find the number of $0 < a \leq 1001$ such that $a, a+1$, and $a+2$ are all relatively prime to 1001.