Algorithms in number theory

Caleb Ji

January 2, 2022

1 Euclidean algorithm

Recall that the fundamental theorem of arithmetic ensures unique factorization into primes.

Theorem 1.1 (Fundamental theorem of arithmetic)**.** *Every positive integer $n > 1$ can be uniquely written (up to reordering) as a product of primes.*

What is wrong with the following proof?

Incomplete proof. By the definition of primes as being only divisible by 1 and itself, we see easily from induction that there exists a factorization of n into primes. To prove uniqueness, assume that there are two different factorizations and cancel out all repeated factors. Then if we are not reduced to $1 = 1$, we have that some prime p divides one side but not the other, which is impossible. □

The issue lies in the last statement. In stating it, we are implicitly assuming that a prime p cannot divide the product of primes other than p. This is of course true, but it is not obvious how to prove it! In fact, this statement is known as Euclid's lemma.

Lemma 1.2 (Euclid's lemma)**.** *An integer $p > 2$ is prime if and only if $p|ab \Rightarrow p|a$ or $p|b$.*

One direction is an easy exercise: if the above condition holds, then p cannot be divisible by any positive integer besides 1 and p. To prove the other direction, we need the Euclidean algorithm and Bezout's lemma.

Proposition 1.3 (Euclidean algorithm)**.** *Let (a, b) denote the gcd of integers a and b and let $b\%a$ denote the remainder when b is divided by a. Then*

$$(a, b) = (a, b\%a).$$

Indeed, adding any multiple of one number to the other will not change the gcd. By repeating this process, the Euclidean algorithm gives a convenient way of computing gcds. Additionally, it gives a proof of Bezout's lemma.

Example 1.4. *We have*

$$\begin{aligned}(37, 14) &= (9, 14)\\ &= (9, 5)\\ &= (4, 5)\\ &= (4, 1)\\ &= 1.\end{aligned}$$

Going in reverse, we have

$$\begin{aligned}1 &= 5 - 4 \\ &= 5 - (9 - 5) = 2 \cdot 5 - 9 \\ &= 2 \cdot (14 - 9) - 9 = 2 \cdot 14 - 3 \cdot 9 \\ &= 2 \cdot 14 - 3(37 - 2 \cdot 14) \\ &= 8 \cdot 14 - 3 \cdot 37.\end{aligned}$$

Lemma 1.5 (Bezout's lemma)**.** *For all nonzero integers a, b, there exist integers x and y such that*

$$ax + by = (a, b).$$

The proof is given by the fact that we can go backwards in the Euclidean algorithm, successively expressing (a, b) as a sum of multiples of the integers used until we get back to a and b.

Now we can prove Euclid's lemma, and thereby, the fundamental theorem of arithmetic.

Proof of Euclid's lemma. Let p be a prime with $p|ab$. We wish to prove that if $p \nmid a$, then $p|b$. Since p is prime, we must have $(a, p) = 1$ and thus by Bezout's lemma we may write $ax+py = 1$. Multiplying both sides by b we obtain $abx + pby = b$. The left hand side is divisible by p, so $p|b$ as desired. □

To summarize, unique factorization rests on the equivalence of two distinct notions of being prime. Actually, the condition of not being written as a product of two smaller integers is generally referred to as **irreduciblity**, while the condition $p|ab \Rightarrow p|a$ or $p|b$ is the definition of being prime.

The question of whether various sets have some sort of unqiue factorization is extremely interesting (and important). Let us now see this in the context of polynomial rings.

Definition 1.6. *Define a **unit** of a ring R (think $R = \mathbb{R}, \mathbb{C}, \mathbb{Z}, \mathbb{Z}/n\mathbb{Z}$ or the polynomial rings over them) to be an element $u \in R$ that divides 1. By definition, this means there is some $v \in R$ such that $uv = 1$.*

Example 1.7. *The units of $\mathbb{Z}$ and $\mathbb{Z}[x]$ are $\{\pm 1\}$. The units of $\mathbb{Z}/8\mathbb{Z}$ are $\{1, 3, 5, 7\}$ but the units of $\mathbb{Z}/8\mathbb{Z}[x]$ include elements such as $4x + 1$, because $(4x + 1)^2 \equiv 1 \pmod 8$. In general, if every nonzero element of R is invertible, then the units of R are the same as the units of $R[x]$ for degree reasons.*

Now we can define irreducible polynomials to be those not divisible by two non-units. For example, $4x \in \mathbb{Z}/8\mathbb{Z}[x]$ is **reducible** since $4x = 4 \cdot x$. Again, we define primes by the property $p(x)|q(x)r(x) \Rightarrow p(x)|q(x)$ or $p(x)|r(x)$. As an exercise, show that primes must be irreducible.

To determine $(p(x), q(x))$ in the case of $\mathbb{R}[x], \mathbb{C}[x]$, an $\mathbb{Z}/p\mathbb{Z}[x]$, we can perform the Euclidean algorithm to continually decrease the degree of the polynomials we're working with until we reach the stage $(r(x), 0)$ in which case we say that $(p(x), q(x)) = r(x)$. Because every nonzero coefficient is invertible in these cases, we can take $r(x)$ to be monic. In fact, invertibility is why we can perform the Euclidean algorithm in the first place. For example, in $\mathbb{Z}/8\mathbb{Z}[x]$ we cannot perform the Euclidean algorithm any further on $(x + 1, 4)$, but in $\mathbb{Z}/7\mathbb{Z}[x]$ we have $(x + 1, 4) = (1, 4) = 1$.

By going backwards as before, we obtain another version of Bezout's lemma.

Lemma 1.8 (Bezout's lemma for polynomials)**.** *Let $p(x), q(x)$ be polynomials over a field F (e.g. $F = \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$). Then there exist polynomials $a(x), b(x) \in F[x]$ such that*

$$a(x)p(x) + b(x)q(x) = (p(x), q(x)).$$

Then as before we see that irreducibles are prime, and thus we have unique factorization of polynomials over fields (i.e. nonzero elements are invertible).

Theorem 1.9 (Wilson's theorem)**.** *Let p be a prime. Then*

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, we have unique factorization of polynoimals. Consider $f(x) = x^{p-1} - 1$. By Fermat's little theorem we know that $1, 2, \ldots, p-1$ are all roots. Since $x - k$ is prime for $k = 1, \ldots, p-1$, by unique factorization we have that each $x - k$ must appear in the prime factorization of $f(x)$. For degree reasons this implies that

$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1)),$$

and by looking at the constant term we are done. □

Remark. The condition of p being prime is necessary; e.g. $x^4 - 1 \neq (x-1)(x-3)(x-5)(x-7) \pmod 8$.

Example 1.10 (ISL 2011 N2)**.** *Consider a polynomial $P(x) = \prod_{j=1}^{9}(x + d_j)$, where $d_1, d_2, \ldots d_9$ are nine distinct integers. Prove that there exists an integer N, such that for all integers $x \geq N$ the number $P(x)$ is divisible by a prime number greater than 20.*

Solution. Suppose the contrary. We see that though the terms in the product get arbitrarily large, their differences remain the same. So the Euclidean algorithm tells us that the gcd of any two of the numbers has to be small, so they should not have the same small set of prime factors.

Motivated by this, we note that there are 9 terms in the product and only 8 primes less than 20. If x is sufficiently large, then each $x + d_j$ must be divisible by one of the 8 primes raised to the power of (say) $\max(\{d_j\}) + 1$. By the Pigeonhole Principle, we must have two distinct terms $x + d_i, x + d_j$ both divisible by $p^{\max(\{d_j\})+1}$. Then by the Euclidean algorithm, we have $p^{\max(\{d_j\})+1} | d_i - d_j$, which is clearly absurd. We are done. □

2 Hensel's lemma

Hensel's lemma provides an answer to the question: if a polynomial has roots modulo p, does it have a root modulo p^k? First, let us analyze when a polynomial defined over a field has multiple roots. We will work in a field K to emphasize that we could either be taking real/complex coefficients, or coefficients in $\mathbb{Z}/p\mathbb{Z}$. Note that by the previous section we have unique factorization in $K[x]$, so in particular concepts like multiplicity of a root are well-defined.

Definition 2.1 ((formal) derivative)**.** *Let $f(x) = \sum_{k=0}^{n} a_k x^k \in K[x]$ be a polynomial over a field. The derivative of $f(x)$ is $\sum_{k=1}^{n} k a_k x^{k-1}$.*

A key property of the derivative is the Leibniz (or product) rule: $(fg)' = f'g + fg'$.

Proposition 2.2. *Let $a \in K$ be a root of a polynomial $f(x) \in K[x]$. Then a is a double root if and only if $f'(a) = 0$.*

Proof. If a is a double root, then write $f(x) = (x-a)^2 g(x)$. Apply the product rule to obtain $f'(a) = 0$. If $f'(a) = 0$, then writing $f(x) = (x-a)g(x)$ and using the product rule gives $g(a) = 0 \Rightarrow x - a | g(a)$. □

Let us now state and prove Hensel's lemma.

Lemma 2.3 (Hensel's lemma, version 1). *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial and let a be an integer satisfying $f(a) \equiv 0 \pmod{p}$ and $f'(a) \neq 0 \pmod{p}$. Then there is a unique infinite integer sequence $a = a_1, a_2, a_3, \ldots$ such that $a_k \equiv a_{k+1} \pmod{p^k}$ for every k and $f(a_k) \equiv 0 \pmod{p^k}$.*

Proof. The idea should be familiar if you've seen Taylor expansions in calculus. We claim that we can write

$$f(x) = f(a) + f'(a)(x-a) + g(a)(x-a)^2$$

for some polynomial $g(x) \in \mathbb{Z}/p\mathbb{Z}[x]$. Indeed, it is easy to check by the criterion above that the polynomial

$$h(x) = f(x) - f(a) - f'(a)(x-a)$$

satisfies $h(a) = h'(a) = 0$, so $h(x)$ can be written as $g(a)(x-a)^2$.

We now proceed by induction. Suppose we have constructed a_k, so $f(a_k) \equiv 0 \pmod{p}^k$ and $a_k \equiv a \pmod{p}$. Then we need to show that there is a unique choice $t \in \{0, 1, \ldots, p-1\}$ such that setting $a_{k+1} = a_k + tp^k$ gives $f(a_{k+1}) \equiv 0 \pmod{p^{k+1}}$. Indeed, with the expression for $f(x)$ above we have

$$\begin{aligned} f(a_k + tp^k) &= f(a_k) + f'(a_k)(tp^k) + g(a)(tp^k)^2 && (1) \\ &\equiv f(a_k) + tf'(a_k)p^k \pmod{p^{k+1}}. && (2) \end{aligned}$$

Since $p^k | f(a_k)$ and $p \nmid f'(a_k)$, we see that there does indeed exist a unique t making it $0 \mod p^{k+1}$. We are done by induction. □

Remark. The natural setting of Hensel's lemma is in the $p-$adic integers $\mathbb{Z}_p$ (or even more general settings). See the theoretical problems if you are interested.

The idea of taking lifts to moduli of higher prime powers is quite common in modular arithmetic. The existence of primitive roots and the lifting the exponent lemma are two well-known examples (see problems).

Example 2.4 (Yufei Zhao handout[1]). *Let N be a positive integer ending in digits 25, and m a positive integer. Prove that for some positive integer n, the rightmost m digits of 5^n and N agree in parity.*

Proof. We use induction; let's assume we've proven that there are infinitely many such n for $m - 1 \geq 2$. Then we have that 5^n matching the first $m-1$ digits of N in parity, and we would like to alter n so that this holds for the first m digits of N. We don't want to change what we have for the first $m-1$ digits, so we note that $5^{n+k} - 5^n = 5^n(5^k - 1)$. Since there are infinitely many such n we have enough powers of 5. By LTE (or something simpler, like the binomial theorem) we have $\nu_2(5^k - 1) = 2 + \nu_2(k)$. Then we see that by picking $2 + \nu_2(k) = m - 1$ we can change the parity of the mth digit, and by setting it equal to m we can keep it. The desired result follows easily. □

[1] http://web.mit.edu/yufeiz/www/olympiad/exponent_lifting_sol.pdf

Example 2.5 (ISL 2010 N4). *Let a, b be integers, and let $P(x) = ax^3 + bx$. For any positive integer n we say that the pair (a, b) is n-good if $n|P(m) - P(k)$ implies $n|m - k$ for all integers m, k. We say that (a, b) is very good if (a, b) is n-good for infinitely many positive integers n.*

(a) Find a pair (a, b) which is 51-good, but not very good.

(b) Show that all 2010-good pairs are very good.

Solution. We see that being n-good is equivalent to $P(x)$ taking every value $\pmod n$ once when evaluated on $\{0, 1, \ldots, n-1\}$. Additionally, by CRT the property of being n-good is multiplicative (for relatively prime moduli).

For part (a), we note that the question is easier if $P(x) = ax^3$, so we can try taking some $51|b$ and just solve this case. Since $(3, 3-1) = (3, 17-1) = 1$ we see that x^3 takes all residues $\pmod 5 1$. Thus $(1, 51k)$ is 51-good. To make sure it is not very good, we can just force it to have a nonzero root. For example, $(1, -51^2)$ works since then $P(51) = P(0) = 0$ and thus $(1, -51^2)$ is not n-good for any $n > 51$.

For part (b), we have $2010 = 2 \cdot 3 \cdot 5 \cdot 67$. We better not have the same nonsense in part (a) happen here which happened because $(3, p-1) = 1$. Thus we focus on 67. We wish to show that if (a, b) is 67-good, then it is 67^k-good for all k. Say we wish to verify that $ax^3 + bx$ takes some value $t \pmod{67^k}$. That is, we need to find a root of $ax^3 + bx - t \pmod{67^k}$. We are given that there is some root $r \pmod{67}$. Then Hensel's lemma finishes the problem as long as the derivative $3ar^2 + b \neq 0 \pmod{67}$. Assume otherwise, so we have $b \equiv -3ar^2 \pmod{67}$; then in this case we have that r is a double root of $ax^3 + bx - t$. Writing $ax^3 + bx - t \equiv a(x-r)^2(x-d) \pmod{67}$, we see that if $r \not\equiv d \pmod{67}$, then $P(r) \equiv P(d) \pmod{67}$, contradiction. If $r \equiv d \pmod 6 7$, then since the quadratic coefficient is 0 we must have $r = 0$. But x^3 is not 67-good, contradiction again. Thus we cannot have $b \equiv -3ar^2 \pmod{67}$, so we are done by Hensel's lemma. □

3 Problems

3.1 Warmup

1. Let $a > 1$ be a positive integer. Show that $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.
2. Let $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ be a polynomial of degree n. Show that f has at most n roots. Does the result hold if p is not prime?
3. Show that for any n, there are infinitely many cubes of the form $2^n a - 9$.
4. Show that the moduli admitting primitive roots are $2, 4, p^k, 2p^k$ for odd primes p.
5. (LTE) Let p be an odd prime with $p|a - b, p \nmid a$. Then if p is odd we have

$$\nu_p(a^n - b^n) = \nu_p(a - b) + \nu_p(n)$$

and if $p = 2$ we have

$$\nu_2(a^n - b^n) = \nu_2\left(\frac{a^2 - b^2}{2}\right) + \nu_2(n).$$

3.2 IMO 1 to IMO 2

1. (USAMO 2003 #1) Prove that for every positive integer n there exists an n-digit number divisible by 5^n all of whose digits are odd.

2. (ISL 2009 N2) A positive integer N is called balanced, if $N = 1$ or if N can be written as a product of an even number of not necessarily distinct primes. Given positive integers a and b, consider the polynomial P defined by $P(x) = (x + a)(x + b)$.

   (a) Prove that there exist distinct positive integers a and b such that all the number $P(1)$, $P(2)$,..., $P(50)$ are balanced.

   (b) Prove that if $P(n)$ is balanced for all positive integers n, then $a = b$.

3. (ISL 2013 N3) Prove that there exist infinitely many positive integers n such that the largest prime divisor of $n^4 + n^2 + 1$ is equal to the largest prime divisor of $(n+1)^4 + (n+1)^2 + 1$.

4. (ISL 2009 N3) Let f be a non-constant function from the set of positive integers into the set of positive integer, such that $a - b$ divides $f(a) - f(b)$ for all distinct positive integers a, b. Prove that there exist infinitely many primes p such that p divides $f(c)$ for some positive integer c.

3.3 IMO 2 to IMO 3

1. (ISL 2015 N3) Let m and n be positive integers such that $m > n$. Define $x_k = \frac{m+k}{n+k}$ for $k = 1, 2, \ldots, n+1$. Prove that if all the numbers $x_1, x_2, \ldots, x_{n+1}$ are integers, then $x_1 x_2 \ldots x_{n+1} - 1$ is divisible by an odd prime.

2. (ISL 2015 N4) Suppose that $a_0, a_1, \cdots$ and $b_0, b_1, \cdots$ are two sequences of positive integers such that $a_0, b_0 \geq 2$ and

$$a_{n+1} = \gcd(a_n, b_n) + 1, \qquad b_{n+1} = \operatorname{lcm}(a_n, b_n) - 1.$$

   Show that the sequence a_n is eventually periodic; in other words, there exist integers $N \geq 0$ and $t > 0$ such that $a_{n+t} = a_n$ for all $n \geq N$.

3. (ISL 2013 N4) Determine whether there exists an infinite sequence of nonzero digits $a_1, a_2, a_3, \cdots$ and a positive integer N such that for every integer $k > N$, the number $\overline{a_k a_{k-1} \cdots a_1}$ is a perfect square.

4. (ISL 2011 N6) Let $P(x)$ and $Q(x)$ be two polynomials with integer coefficients, such that no nonconstant polynomial with rational coefficients divides both $P(x)$ and $Q(x)$. Suppose that for every positive integer n the integers $P(n)$ and $Q(n)$ are positive, and $2^{Q(n)} - 1$ divides $3^{P(n)} - 1$. Prove that $Q(x)$ is a constant polynomial.

3.4 Theoretical problems

1. (Unique factorization domains) Recall that unique factorization comes from the assertion that irreducibles are prime, which came from existence of a Euclidean function. Given a ring R, define a Euclidean function to be a function $N : R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ such that for $a, b \in R$ (with $b \neq 0$), we can write $a = bq + r$ with $N(r) < N(b)$ or $r = 0$. This allows us to perform the Euclidean algorithm, which leads to Bezout's lemma, which leads to unique factorization. (N.B. It is not *necessary* to be Euclidean to be a UFD.)

   (a) Consider the ring $R = \mathbb{Z}[i] \coloneqq \{a + bi | a, b \in \mathbb{Z}\}$ with the norm function $N(a + bi) = a^2 + b^2$. Show that N is a Euclidean function, thereby showing that $\mathbb{Z}[i]$ is a UFD.

   (b) Find the primes of $\mathbb{Z}[i]$.

   (c) Define the norm function on $\mathbb{Z}[\sqrt{d}]$ by $N(a + b\sqrt{d}) = a^2 - db^2$. Use it to show that $\mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{3}]$ are Euclidean.

2. (p-adic numbers) We can define $\mathbb{Z}_p$, the p-adic integers, to be all sequences of the form $\sum_{i=0}^{\infty} c_i p^i$ for residues $c_i \in \{0, 1, \ldots, p-1\}$. Alternatively, by taking partial sums we may define them as sequences $a_1, a_2, \ldots$ where $a_i \in \mathbb{Z}/p^i\mathbb{Z}$ satisfying $a_i \equiv a_{i+1} \pmod{p}^i$. Another way of phrasing this is that $\mathbb{Z}_p$ is the inverse limit

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

   The p-adic integers form a ring that include the integers. Moreover, there is a canonical projection map to $\mathbb{Z}/p\mathbb{Z}$ by simply taking a_1. We can restate Hensel's lemma (slightly generalized) as follows: if a polynomial $f(x) \in \mathbb{Z}_p[x]$ has a root $\overline{r}$ in its reduction to $\overline{f}(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ and $\overline{f}'(r) \neq 0$, then $\overline{r}$ can be uniquely lifted to a root $r \in \mathbb{Z}_p$.

   Prove the following more general version of Hensel's lemma: if a polynomial $f \in \mathbb{Z}_p[x]$ factors as $\overline{f} = \overline{g}\overline{h}$ into relatively prime polynomials $\overline{g}, \overline{h} \in \mathbb{Z}/p\mathbb{Z}[x]$, then $\overline{g}, \overline{h}$, can be uniquely lifted to $g, h \in \mathbb{Z}_p[x]$ such that $f = gh$.