Numbers Made Dumber

Rohan Baijal
Vivek Kumar Singh
Yatharth Goswami

Week 2

19-04-2021

1.1 Prime Numbers and prime-power factorisations

An integer $p > 1$ is said to be prime if the only positive divisors of are 1 and p itself. Note that 1 is not prime. The smallest prime is 2, and all the other primes (such as $3, 5, 7, 11, \dots$) are odd. An integer $n > 1$ which is not prime (such as $4, 6, 8, 9, \dots$) is said to be composite; such an integer has the form $n = ab$ where $1 < a < n$ and $1 < b < n$.

Lemma 1.1.1. *Let p be prime, and let a and b be any integers. Then*

1. *either p divides a, or a and p are coprime;*
2. *if p divides ab, then p divides a or p divides b.*

Proof.

1. By its definition, $gcd(a, p)$ is a positive divisor of p, so it must be 1 or p since p is prime. If $gcd(a, p) = p$, then since $gcd(a, p)$ divides a we have $p|a$; if $gcd(a, p) = 1$ then a and p are coprime.
2. Let $p|ab$. If p does not divide a then part (a) implies that $gcd(a, p) = 1$. Now Bezout's identity gives $1 = au+pv$ for some integers u and v, so $b = aub+pvb$. By our assumption, p divides ab and hence divides aub; it clearly divides pvb, so it also divides b, as required. □

Both parts of this result can fail if p is not prime: take $p = 4, a = 6$ and $b = 10$, for instance. Lemma 2.1(b) can be extended to products of any number of factors:

Corollary 1.1.1.1. *If p is prime and p divides $a_1...a_k$, then p divides a_i for some i.*

Proof. We use induction on k. If $k = 1$ then the assumption is that $p|a_1$, so the conclusion is automatically true (with $i = 1$). Now assume that $k > 1$ and that the result is proved for all products of $k - 1$ factors a_i. If we put $a = a_1...a_k - 1$ and $b = a_k$, then $a_1...a_k = ab$ and so $p|ab$. By Lemma 2.1(b), it follows that $p|a$ or $p|b$. In the first case we have $p|a$ or $p|b$. In the first case we have $p|a_1 \dots a_{k-1}$, so the induction hypothesis implies that $p|a_i$ for some $i = 1, \dots, k - 1$; in the second case we have $p|a_k$. Thus in either case $p|a_i$ for some i, as required. □

The next result, known as the *Fundamental Theorem of Arithmetic*, explains why prime numbers are so important: they are the basic building blocks out of which all integers can be constructed.

Theorem 1.1.2. *Each integer $n > 1$ has a prime-power factorisation*

$$n = p_1^{e_1} \dots p_k^{e_k}$$

where $p_i, \dots, p_k$ are distinct primes and $e_i, \dots, e_k$ are positive integers; this factorisation is unique, apart from permutations of the factors.

Proof. First we use the principle of strong induction to prove the existence of prime-power factorisations. Since we are assuming that $n > 1$, the induction starts with $n = 2$. As usual, this case is easy: the required factorisation is simply $n = 2^1$. Now assume that $n > 2$ and that every integer strictly between 1 and n has a prime-power factorisation. If n is prime then $n = n^1$ is the required factorisation of n, so we can assume that n is composite, say $n = ab$ where $1 < a, b < n$. By the induction hypothesis, both a and b have prime-power factorisations, so by substituting these into the equation $n = ab$ and then collecting together powers of each prime p_i we get a prime-power factorisation of n.
Now we prove uniqueness. Suppose that n has prime-power factorisations

$$n = p_1^{e_1} \dots p_k^{e^k} = q_1^{f_1} \dots q_l^{f^l}$$

where $p_1, ..., p_k$ and $q_1, ..., q_l$ are two sets of distinct primes, and the exponents e_i and f_j are all positive. The first factorisation shows that $p_1|n$, so Corollary 2.2 (applied to the second factorisation) implies that $p_1|q_j$ for some $j = 1, ..., l$. By permuting (or renumbering) the prime-powers in the second factorisation we may assume that $j = 1$, so $p_1|q_l$. Since q_i is prime, it follows that $p_1 = q_l$, so cancelling this prime from the two factorisations we get

$$p_1^{e_1-1} \dots p_k^{e_k} = q_1^{f_1-1} \dots q_l^{f_l}$$

We keep repeating this argument, matching primes in the two factorisations and then cancelling them, until we run out of primes in one of the factorisations. If one factorisation runs out before the other, then at that stage our reduced factorisations express 1 as a product of primes p_i or p_j, which is impossible since $p_i, q_j > 1$. It follows that both factorisations run out of primes simultaneously, so we must have cancelled the e_i copies of each p_i with the same number (f_i) of copies of q_i; thus $k = l$, each $p_i = q_i$ (after permuting factors), and each $e_i = f_i$, so we have proved uniqueness. □

Theorem 1.1.2 allows us to use prime-power factorisations to calculate products, quotients, powers, greatest common divisors and least common multiples. Suppose that integers a and b have factorisations

$$a = p_1^{e_1} \dots p_k^{e_k} \text{ } and \text{ } b = p_1^{f_1} \dots p_k^{f_k}$$

(where we have $e_i, f_i \geq 0$ to allow for the possibility that some primes p_i may divide one but not both of a and b). Then we have

$$\begin{aligned} ab &= p_1^{e_1+f_1} \dots p_k^{e_k+f_k} \\ a/b &= p_1^{e_1-f_1} \dots p_k^{e_k-f_k} \\ a^m &= p_1^{me_1} \dots p_k^{me_k} \\ gcd(a,b) &= p_1^{min(e_1,f_1)} \dots p_k^{min(e_k,f_k)} \\ lcm(a,b) &= p_1^{max(e_1,f_1)} \dots p_k^{max(e_k,f_k)} \end{aligned}$$

where min(e, f) and max(e, f) are the minimum and maximum of e and f. Unfortunately, finding the factorisation of a large integer can take a very long time!
The following notation is often useful: if p is prime, we write $p^e||n$ to indicate that p^e is the highest power of p dividing n, that is, p^e divides n but p^{e+1} does not. The preceding results show that if $p^e||a$ and $p^f||b$ then $pe = f||ab$, $p^{e-f}||a/b$ (if $b|a$), $p^{me}||a^m$, etc.

Lemma 1.1.3. *If $a_1 \dots, a_r$ are mutually coprime positive integers, and $a = a_1 \dots a_r$ is an m-th power for some integer $m \geq 2$, then each a_i is an m-th power.*

Proof. It follows from the above formula for a^m that a positive integer is an m-th power if and only if the exponent of each prime in its prime-power factorisation is divisible by m. If $a = a_1 ... ar$, where the factors a_i are mutually coprime, then each prime power p^e appearing in the factorisation of any a_i also appears as the full power of p in the factorisation of a; since a is an m-th power, e is divisible by m, so a_i is an m-th power. □

We can use prime-power factorisations to generalise the classic result that $\sqrt{2}$ is irrational. A rational number is a real number of the form a/b, where a and b are integers and $b \neq 0$; all other real numbers are irrational.

Corollary 1.1.3.1. *If a positive integer m is not a perfect square, then $\sqrt{m}$ is irrational.*

Proof. It is sufficient to prove the contrapositive, that if $\sqrt{m}$ is rational then m is a perfect square. Suppose that $\sqrt{m} = a/b$ where a and b are positive integers. Then

$$m = \frac{a^2}{b^2}$$

If a and b have prime-power factorisations

$$a = p_1^{e_1} \dots p_k^{e_k} \; and \; b = p_1^{f_1} \dots p_k^{f_k}$$

as above, then

$$m = p_1^{2_1^e - 2f_1} \dots p_k^{2e_k - 2f_k}$$

must be the factorisation of m. Notice that every prime p_i appears an even number of times in this factorisation, and $e_i - f_i \geq 0$ for each i, so

$$m = (p_1^{e_1 - f_1} \dots p_k^{e_k - f_k})^2$$

is a perfect square. □

1.2 Distribution of Primes

There are infinitely many primes! This is one of the most oldest and attractive theorems in Maths.

Theorem 1.2.1. *There are infinitely many primes.*

Proof. The proof is by contradiction: we assume that there are only finitely many primes, and then we obtain a contradiction from this, so it follows that there must be infinitely many primes.
Suppose then that the only primes are $p_1, p_2, ..., p_k$. Let

$$m = p_1 p_2 ... p_k + 1. \tag{1.1}$$

Since m is an integer greater than 1, the Fundamental Theorem of Arithmetic implies that it is divisible by some prime p (this includes the possibility that $m = p$). By our assumption, this prime p must be one of the primes $p_1, p_2, ..., p_k$, so p divides their product $p_1 p_2 ... p_k$. Since p divides both m and $p_1 p_2 ... p_k$ it divides $m - p_1 p_2 ... p_k = 1$, which is impossible. We deduce that our initial assumption was false, so there must be infinitely many primes.
□

Corollary 1.2.1.1. *The n-th prime p_n satisfies $p_n \leq 2^{2^{n-1}} \; \forall n \geq 1$.*
By plugging in some numbers, you will realise that this is a very weak estimate :p

Proof. We use strong induction on n. The result is true for n = 1, since $p_1 = 2 = 2^{2^0}$. Now assume that the result is true for each $n = 1, 2, ..., k$. As in the proof of Theorem 1.2.1, $p_1 p_2 ... p_k + 1$ must be divisible by some prime p; this prime cannot be one of $p_1, p_2, ..., p_k$, for then it would divide 1, which is impossible. Now this new prime p must be at least as large as the $(k+1)$-th prime p_{k+1} so

$$p_{k+1} \leq p \leq p_1 p_2 ... p_k + 1 \leq 2^{2^0}.2^{2^1}...2^{2^{k-1}} + 1 = 2^{2^k - 1} + 1 \leq 2^{2^k} \tag{1.2}$$

□

For any real number $x > 0$, let $\pi(x)$ denote the number of primes $p \leq x$; then $\pi(1) = 0, \pi(2) = 1, \pi(10) = 4$.

Corollary 1.2.1.2. $\pi(x) \geq \lfloor log_2(log_2(x)) \rfloor + 1$.

Proof. $\lfloor log_2(log_2(x)) \rfloor + 1$ is the largest integer n such that $2^{2^{n-1}} \leq x$. By Corollary 1.2.1.1, there are atleast n primes $p_1, p_2, ...p_n \leq 2^{2^{n-1}}$. These primes are all less than or equal to x, so $\pi(x) \geq \lfloor log_2(log_2(x)) \rfloor + 1$. □

As mentioned earlier, this is a very weak bound. Later Gauss gave a better approximation for this

$$\frac{\pi(x)}{x/lnx} \to 1 \ as \ x \to \infty \tag{1.3}$$

Theorem 1.2.2. *There are infinitely many primes of the form 4q + 3.*

Proof. The proof is by contradiction. Suppose that there are only finitely many primes of this form, say $p_1, ...p_k$. Let $m = 4p_1...p_k - 1$, so m also has the form $4q + 3$ (with $q = p_1 p_2 ... p_k - 1$). Since m is odd, so is each prime p dividing m, so p has the form $4q + 1$ or $4q + 3$ for some q. If each such p has the form $4q + 1$, then m (being a product of such integers) must also have this form, which is false. Hence m must be divisible by at least one prime p of the form $4q + 3$. By our assumption, $p = p_i$ for some i, so p divides $4p_1...p_k - m = 1$, which is impossible. This contradiction proves the result. □

There is a nice general result but we will not go into the proof.

Theorem 1.2.3. *If a and b are coprime integers then there are infinitely many primes of the form $aq + b$.*

1.3 Fermat and Mersenne Primes

In order to find specific examples of primes, it seems reasonable to look at integers of the form $2m \pm 1$, since many small primes, such as $3, 5, 7, 17, 31, \ldots$, have this form.

Lemma 1.3.1. *If $2^m + 1$ is prime, then $m = 2^n$ for some integer $n \geq 0$.*

Proof. We prove the contrapositive, that if m is not a power of 2 then $2m + 1$ is not prime. If m is not a power of 2, then m has the form $2^n q$ for some odd $q > 1$. Now the polynomial $f(t) = t^q + 1$ has a root $t = -1$, so it is divisible by $t + 1$; this is a proper factor since $q > 1$, so putting $t = x^{2^n}$ we see that the polynomial $g(x) = f(x^{2^n}) = x^m + 1$ has a proper factor $x^{2^n} + 1$. Taking $x = 2$ we see that $2^{2^n} + 1$ is a proper factor of the integer $g(2) = 2^m + 1$, which cannot therefore be prime. □

Numbers of the form $F_n = 2^{2^n} + 1$ are called Fermat numbers, and those which are prime are called Fermat primes. Fermat conjectured that F_n is prime for every $n \neq 0$. For $n = 0, ..., 4$ the numbers $F_n = 3, 5, 17, 257, 65537$ are indeed prime, but in 1732 Euler showed that the next Fermat number

$$F_5 = 2^{2^5} + 1 = 641 \times 6700417$$

is composite. The Fermat numbers have been studied intensively, often with the aid of computers, but no further Fermat primes have been found. It is conceivable that there are further Fermat primes (perhaps infinitely many) which we have not yet found, but the evidence is not very convincing. These primes are important in geometry: in 1801 Gauss showed that a regular polygon with k sides can be constructed by ruler-and-compass methods if and only if $k = 2^e p_1 \dots p_r$ where $p_1, \dots, p_r$ are distinct Fermat primes.

Even if not many of the Fermat numbers F_n turn out to be prime, the following result shows that their factors include an infinite set of primes:

Lemma 1.3.2. *Distinct Fermat numbers F_n are mutually coprime.*

Proof. Let $d = gcd(F_n, F_{n+k})$ be the greatest common divisor of two Fermat numbers F_n and F_{n+k} , where $k > 0$. The polynomial $x^{2^k} - 1$ has a root $x = -1$, so it is divisible by $x + 1$. Putting $x = 2^{2^n}$ we see that F_n divides $F_{n+k} - 2$, so d divides 2 and hence d is 1 or 2. Since all Fermat numbers are odd, $d = 1$. □

Theorem 1.3.3. *If $m > 1$ and $a^m - 1$ is prime, then $a = 2$ and m is prime.*

Proof. Left as an exercise to the reader. □

Integers of the form $2^p - 1$, where p is prime, are called Mersenne numbers, after Mersenne who studied them in 1644; those which are prime are called Mersenne primes. M_p is not prime for every prime p.

1.4 Primality-testing and factorisation

There are two practical problems which arise from the theory we have considered in this chapter:

1. How do we determine whether a given integer n is prime?
2. How do we find the prime-power factorisation of a given integer n?

In relation to the first problem, known as *primality-testing*, we have:

Lemma 1.4.1. *An integer $n > 1$ is composite if and only if it is divisible by some prime $p \leq \sqrt{n}$.*

Proof. If n is divisible by such a prime p, then since $1 < p \leq \sqrt{n} < n$ it follows that n is composite. Conversely, if n is composite then $n = ab$ where $1 < a < n$ and $1 < b < n$; at least one of a and b is less than or equal to $\sqrt{n}$ (if not, $ab > n$), and this factor will be divisible by a prime $p \leq \sqrt{n}$, which then divides n. □

In decimal notation we write a positive integer n in the form $a_k ak - 1 ... a_1 a_0$, meaning that

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$$

where $a_0, ..., a_k$ are integers with $0 \leq a_i \leq 9$ for all i, and $ak \neq 0$. From this, we see that n is divisible by 2 if and only if a_0 is divisible by 2, that is, $a_0 = 0, 2, 4, 6or8$; similarly, n is divisible by 5 if and only if $a_0 = 0or5$. With a little more ingenuity, we can also get tests for divisibility by 3 and 11. If we expand $10^i = (9 + 1)^i$ by the Binomial Theorem we get an integer of the form $9q + 1$; by doing this for each $i = 1, ..., k$ we see that

$$n = 9m + a_k + a_{k-1} + \cdots + a_1 + a_0$$

for some integer m, so n is divisible by 3 if and only if the sum of the digits is divisible by 3. Similarly by putting $10^i = (11 - 1)^i = 11q + (-1)^i$ we see that

$$n = 11m + (-1)^k a_k + \cdots - a_1 + a_0$$

so n is divisible by 11 if and only if the alternating sum of its digits is divisible by 11.

This method of primality-testing is effective for fairly small integers n, since there are not too many primes p to consider, but when n becomes large it is very time-consuming: by the Prime Number Theorem, the number of primes $p \leq \sqrt{n}$ is given by

$$\pi(\sqrt{n}) \approx \frac{\sqrt{n}}{ln(\sqrt{n})} = \frac{2\sqrt{n}}{ln(n)}$$

In cryptography (the study of secret codes), one regularly uses integers with several hundred decimal digits; if $n \approx 10^100$, for example, then this method would involve testing about $8x10^47$ primes p, and even the fastest available supercomputers would take far longer than the current estimate for the age of the universe (about 15 billion years) to complete this task! Fortunately there are alternative algorithms (using some very sophisticated number theory) which will determine primality for very large integers much more efficiently. Some of the fastest of these are probabilistic algorithms, such as the Solovay-Strassen test, which will always detect a prime integer n, but which may incorrectly declare a composite number n as being prime; this may appear to be a disastrous fault, but in fact the probability of such an incorrect outcome is so low (far lower than the probability of a computational error due to a machine fault) that for most practical purposes these tests are very reliable.

The Sieve of Eratosthenes is a systematic way of compiling a list of all the primes up to a given integer N. First we list the integers $2, 3, \ldots, N$ in increasing order. Then we underline 2 (which is prime) and cross out all the proper multiples $4, 6, 8, \ldots$ of 2 in the list (since these are composite). The first integer which is neither underlined nor crossed out is 3: this is prime, so we underline it and then cross out all its proper multiples $6, 9, 12, \ldots$ At the next stage we underline 5 and cross out $10, 15, 20, \ldots$. We continue like this until every integer in the list is either underlined or crossed out. At each stage, the first integer which is neither underlined nor crossed out must be prime, for otherwise it would have been crossed out, as a proper multiple of an earlier prime; thus only primes are underlined, and conversely, each prime in the list is eventually underlined at some stage, so when the process terminates the underlined numbers are precisely the primes $p \leq N$ (We can actually stop earlier, when the proper multiples of all the primes $p \leq \sqrt{N}$ have been crossed out, since Lemma 1.4.1 implies that every remaining integer in the list must be prime.)

Our second practical problem, factorisation, is apparently much harder than primality-testing. (It cannot be any easier, since the prime-power factorisation of an integer immediately tells us whether or not it is prime.) In theory we could factorise any integer n by testing it for divisibility by the primes $2, 3, 5, \ldots$ until a prime factor p is found; we then replace n with n/p

and continue this process until a prime factor of n/p is found; eventually, we obtain all the prime factors of n, with their multiplicities. This algorithm is quite effective for small integers, but when n is large we meet the same problem as in primality-testing, that there are just too many possible prime factors to consider. There are, of course, more subtle approaches to factorisation, but at present the fastest known algorithms and computers cannot, in practice, factorise integers several hundred digits long (though nobody has yet proved that an efficient factorisation algorithm will never be found). A very effective cryptographic system (known as the RSA public key system, after its inventors Rivest, Shamir and Adleman, 1978) is based on the fact that it is relatively easy to calculate the product $n = pq$ of two very large primes p and q, while it is extremely difficult to reverse this process and obtain the factors p and q from n. We will examine this system in more detail later in the project.