MATH10040
Chapter 2: Prime and relatively prime numbers

1. Prime numbers

Recall the basic definition:

Definition 1.1. *Recall that a positive integer is said to be* prime *if it has precisely two positive divisors (which are necessarily* 1 *and the number itself)*

An integer greater than 1 *which is not prime is said to be* composite*.*

Thus a prime number p is a number greater than 1 which has no factorizations other that the trivial factorizations $p = 1 \cdot p = p \cdot 1 = (-1) \cdot (-p) = (-p) \cdot (-1)$.

By definition, a (positive) composite number n admits at least one nontrivial factorization $n = rs$ where $2 \leq r, s \leq n - 1$.

Given a large integer, it can be a difficult task to determine whether it is prime or composite.[1]

With not-too-large integers the following observation helps:

Lemma 1.2. *Let n be a composite number. Then n has a prime divisor p satisfying $2 \leq p \leq \sqrt{n}$.*

Proof. We have $n = rs$ with $2 \leq r, s \leq n - 1$. But, by a previous result, either $r \leq \sqrt{n}$ of $s \leq \sqrt{n}$. Without loss of generality, $r \leq \sqrt{n}$. Now take p to be any prime divisor of r. □

Thus, if an integer n has no prime divisor less than or equal to $\sqrt{n}$, it cannot be composite and so must be prime.

Example 1.3. *Is the number* 211 *prime?*

Solution: *If* 211 *were composite it would have a prime divisor smaller than* $\sqrt{211} < 15$. *Thus one of the primes* $2, 3, 5, 7, 11, 13$ *would divide it. Since none of these divide it, it must be prime.*

[1]

> The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic.

C.F Gauss, Disquisitiones Arithmeticae, 1801

There is a polynomial time algorithm (i.e. an efficient computer programme) – discovered only recently by an Indian computer scientist and two undergraduate students – to determine whether a given integer is prime or not. Such an algorithm is said to be a *test for primality*.

Amazingly, the algorithm can determine that a number is composite *without finding any factors*. (We will see later in the course how this is possible.)

In fact, it turns out that the problem of factoring large integers (eg with several hundred digits) – *even when we can prove that they are not prime* – is still intractable. There is no known efficient algorithm or programme for finding the factors of a large composite integer. Given a 300-hundred digit integer which is the product of two 150-digit prime numbers, all the supercomputers in the world running from now until the death of the sun will not find these prime factors using current techniques (unless the factors are of some very particular form). In fact the security of the modern cryposystems that are used in banking and national security rely on this fact. (More on this later in the course.)

2. Relatively prime numbers

Definition 2.1. *Two nonzero integers a and b are said to be* relatively prime *if $(a, b) = 1$.*

Example 2.2. 12 *and* 35 *are relatively prime.* 12 *and* 15 *are not relatively prime.*

Remark 2.3. *If p is prime and $a \in \mathbb{Z}$, then the only positive divisors of p are 1 and p and hence either $(a, p) = 1$ or $(a, p) = p$. In the first case, a and p are relatively prime. In the second, $p|a$.*

Thus, when p is prime, either $(a, p) = 1$ or $p|a$.

Example 2.4. 4 *and* 6 *are not relatively prime. Observe that* $4|60 = 10 \cdot 6$ *but* $4 \not| 10$ *and* $4 \not| 6$.

The following is the key property of relatively prime numbers, which we will use repeatedly throughout the remainder of the course:

Theorem 2.5. *Suppose that $(a, b) = 1$ and that $a|bc$. Then $a|c$.*

Proof. Since $(a, b) = 1$, there exist $s, t \in \mathbb{Z}$ with $1 = as + bt$. Since $a|bc$ there exists $n \in \mathbb{Z}$ with $bc = na$.

Thus

$$c = c \cdot 1 = c \cdot (as + bt) = a(sc) + (bc)t = a(sc) + nat = a \cdot (sc + nt)$$

is a multiple of a. □

Corollary 2.6. *Let p be a prime number and suppose that $p|ab$. Then $p|a$ or $p|b$.*

Proof. If $p|a$ we are done. Otherwise, $(a, p) = 1$ (see remarks above) and hence $p|b$ by Theorem 2.5. □

Corollary 2.7. *If p is prime and $p|a^2$ then $p|a$.*

Proof. Take $a = b$ in Corollary 2.6. □

Example 2.8. *Of course, the corresponding statement for composite numbers is usually false. For example $12|6^2$ but $12 \not| 6$.*

We can generalize these last two corollaries:

Corollary 2.9. *Let p be a prime number. Suppose that $a_1, \ldots, a_n$ are integers and that $p|a_1a_2 \cdots a_n$. Then $p|a_i$ for some $i \leq n$.*

Proof. We'll prove this by induction on $n \geq 2$.[2]

The case $n = 2$ is precisely Corollary 2.6.

Suppose now that the result is true for some $n \geq 2$ and that we are given $n + 1$ integers $a_1, \ldots, a_n, a_{n+1}$ and that $p|a_1 \cdots a_{n+1}$.

Take $a = a_1 \cdots a_n$ and $b = a_{n+1}$ in Corollary 2.6. It follows that $p|a_1 \cdots a_n$ or $p|a_{n+1}$. By our inductive hypothesis, it follows that $p|a_i$ for some $i \leq n$ or $p|a_{n+1}$. □

Corollary 2.10. *If p is a prime number and if $p|a^n$, then $p|a$.*

Proof. Let $a_1 = a_2 = \cdots = a_n = a$ in Corollary 2.9. □

3. Irrationality of certain roots

The ancient sect of Pythagoreans (ca 400BC) were convinced that all essential facts about the universe were determined by whole numbers and their ratios. For example, they discovered the importance of ratios of musical string lengths in the creation of harmonies. Thus it caused them some difficulties that, try as they might, they could not find a pair of whole numbers m and n such that the diagonal of a unit square is exactly equal to m/n. If d is the length of the diagonal of a square of side 1, then (by Pythagoras's Theorem), we have $d^2 = 1^2 + 1^2 = 2$; in modern notation, $d = \sqrt{2}$. Eventually, one of their number (Hippasus of Metapontum) discovered the shocking truth: there are naturally ocurring magnitudes which cannot be expressed as a ratio of whole numbers. The diagonal of a unit square is one such number:

[2] So the statement 'P(n)' is: Given any n integers $a_1, \ldots, a_n$, if $p|a_1a_2 \cdots a_n$ then $p|a_i$ for some i

Lemma 3.1. *$\sqrt{2}$ is not a rational number.*

Proof. Suppose *for the sake of contradiction* that $\sqrt{2}$ is rational. Then we can write this rational number in reduced form; there are nonzero integers a, b satisfying $(a, b) = 1$ and $\sqrt{2} = a/b$.

Squaring we get

$$2 = \frac{a^2}{b^2} \quad \Longrightarrow \quad 2b^2 = a^2.$$

This equation shows that $2|a^2$ (i.e. a^2 is even). By Corollary 2.7 with $p = 2$ it follows that $2|a$ (i.e. a is even). Thus $a = 2c$ for some integer c.

Then

$$2b^2 = a^2 = (2c)^2 = 4c^2 \quad \Longrightarrow \quad b^2 = 2c^2.$$

But this implies that b^2 is even, and hence that b is even by the same argument as for a.

Thus $2|a$ and $2|b$; a *contradiction*, since $(a, b) = 1$. □

In fact, this proof can be applied equally to any prime number:

Theorem 3.2. *Let p be a prime number. Then $\sqrt{p}$ is irrational.*

Proof. Suppose *for the sake of contradiction* that $\sqrt{p}$ is rational. Then we can write this rational number in reduced form; there are nonzero integers a, b satisfying $(a, b) = 1$ and $\sqrt{p} = a/b$.

Squaring we get

$$p = \frac{a^2}{b^2} \quad \Longrightarrow \quad pb^2 = a^2.$$

This equation shows that $p|a^2$. By Corollary 2.7 it follows that $p|a$. Thus $a = pc$ for some integer c.

Then

$$pb^2 = a^2 = (pc)^2 = p^2c^2 \quad \Longrightarrow \quad b^2 = pc^2.$$

But this implies that $p|b^2$, and hence that $p|b$ by the same argument as for a.

Thus $p|a$ and $p|b$; a *contradiction*, since $(a, b) = 1$. □

Remark 3.3. *It follows that we have a list of infinitely many irrational numbers:*

$$\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \ldots$$

and we can find many more:

For example the number

$$\phi := \frac{1+\sqrt{5}}{2}$$

was particular revered by the Pythagoreans. It is called the golden ratio *or* golden section. *(It arises as the ratio of the diagonal to the side of a regular pentagon.)*

It is easy to see that ϕ is irrational: Suppose FTSOC *that ϕ were rational. Then $2\phi = 1+\sqrt{5}$ would be rational, and hence $2\phi - 1 = \sqrt{5}$ would be rational – a contradiction.*

Exercise 3.4. *Let p be a prime and $n > 1$. Prove that $\sqrt[n]{p}$ is not rational.*

4. Solving the equation $ax + by = c$

Let a, b, c be nonzero integers. In this section we describe how to find all *integer* solutions x and y of the equation $ax + by = c$. (The equation $ax + by = c$ is of course the equation of a straight line in the cartesian plane $\mathbb{R}^2$. The subset $\mathbb{Z}^2$ of $\mathbb{R}^2$ consists of all those points whose coordinates are integers. It is called the *integer lattice* in $\mathbb{R}^2$. Draw a picture of (part of) this lattice. Geometrically, what we are doing is finding the points in the integer lattice through which the line $ax + by = c$ passes.)

We have already seen in Chapter 1 that a necessary and sufficient condition for the equation $ax + by = c$ to have a solution is that $(a, b)|c$. Thus, if $(a, b) \not| c$, there are *no* points on the line $ax+by = c$ with integer coordinates.

So we may assume that c is a multiple of $g = (a, b)$. Thus there are integers a', b', c' such that $a = a'g, b = b'g$ and $c = c'g$. Recall furthermore that $(a', b') = 1$ in these circumstances. Finally, observe that the equations $ax + by = c$ and $a'x + b'y = c'$ have the same integer solutions (since the second is obtained from the first by dividing across by g). Thus it's enough to figure out how to solve the second equation. In other words we just have to figure out how to find integer solutions of equations $ax + by = c$ where $(a, b) = 1$ (replacing a, b, c by a', b', c' if necessary).

Recall from Chapter 1, that we find *one* solution of the equation as follows. Use Euclid's algorithm to find $s, t \in \mathbb{Z}$ satisfying $as+bt = 1$. Then multiply across by c: $c = a(cs) + b(ct)$. So $x = cs, y = ct$ is a solution.

Lemma 4.1. *Suppose that $(a, b) = 1$ and that $x = s, y = t$ is an integer solution of the equation*

$$ax + by = c. \tag{1}$$

(1) *For any $m \in \mathbb{Z}$, $x = s + mb, y = t - ma$ is also a solution.*

(2) *This accounts for all integer solutions of (1): If $x = S, y = T$ is any solution, then there exists $m \in \mathbb{Z}$ with $S = s + mb, T = t - ma$. Thus the general solution of (1) is*

$$x = s + mb,\ y = t - ma \qquad m \in \mathbb{Z}.$$

Proof. (1) Given that $as + bt = c$, we have $a(s + mb) + b(t - ma) = as + mab + bt - mab = as + bt = c$.

(2) Let $x = S, y = T$ be a solution. Then

$$as + bt = c = aS + bT \quad \Longrightarrow \quad a(S - s) = b(t - T).$$

It follows that $a|b(t-T)$ and, since $(a, b) = 1$, we deduce that $a|t-T$; i.e. $t - T = ma$ for some integer m and hence $T = t - ma$.

But then $a(S - s) = b(t - T) = b \cdot (ma) \Longrightarrow S - s = mb \Longrightarrow S = s + mb$.

□

Example 4.2. *Find all integer solutions of the equation*

$$57x + 31y = 3.$$

Find the solution with the smallest positive value for x.

Solution: *First use Euclid's algorithm:*

$$\begin{aligned} 57 &= 31 + 26 \\ 31 &= 26 + 5 \\ 26 &= 5 \cdot 5 + 1. \end{aligned}$$

So

$$\begin{aligned} 1 &= 26 - 5 \cdot 5 \\ &= 26 - 5 \cdot (31 - 26) = 6 \cdot 26 - 5 \cdot 31 \\ &= 6 \cdot (57 - 31) - 5 \cdot 31 = 6 \cdot 57 - 11 \cdot 31. \end{aligned}$$

Multiplying across by 3 *gives*

$$3 = 57 \cdot 18 - 31 \cdot 33.$$

So $x = 18, y = -33$ is one solution. By the Lemma, the general solution is

$$x = 18 + 31m, y = -33 - 57m, \quad m = \ldots, -2, -1, 0, 1, 2, \ldots$$

(In other words, the solutions are the pairs

$$\ldots, (-44, 81), (-13, 24), (18, -33), (49, -90), (80, -147), \ldots)$$

Since any solution x must differ from 18 *by a multiple of* 31*,* 18 *is the smallest possible positive value of x.*

Example 4.3. *Find all integer solutions of the equation*

$$72x + 51y = 15.$$

Solution: *Since* $(72, 51) = 3$ *and since* $3|15$*, we divide across by* 3 *to get the equation*

$$24x + 17y = 5.$$

Using Euclid's algorithm we find that $1 = 24 \cdot 5 - 17 \cdot 7$ *and hence* $5 = 24 \cdot 25 - 17 \cdot 35$*.*

Thus $x = 25, y = -35$ *is a solution. Hence the general solution is*

$$x = 25 + 17m, y = -35 - 24m, \quad m \in \mathbb{Z}$$

(So a smaller solution is $x = 25 - 17 = 8, y = -35 + 24 = -11$*, on taking* $m = -1$*.)*

5. The Fundamental Theorem of Arithmetic

We have seen that every number can be expressed as a product of prime numbers.

Example 5.1. $21 = 3 \cdot 7$*.*

$30 = 2 \cdot 3 \cdot 5$*.*

$75 = 3 \cdot 5 \cdot 5 = 3 \cdot 5^2$

$180 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^2 \cdot 3^2 \cdot 5$*.*

etc

However it is not immediately obvious that this can be done in only one way. For example, is the following equation true or false:

$3^{58} \cdot 11^{12} = 5^{42} \cdot 13^{13}$.

In this case, we can easily use the properties of prime numbers to show that the equation must be false: Suppose FTSOC that it were true. Then $3|3^{58} \cdot 11^{12} \implies 3|5^{42} \cdot 13^{13}$. But this latter implies $3|5$ or $3|13$ by Corollary 2.9 – a contradiction.

How about the following equation?:

$3^{15} \cdot 7^{20} \cdot 11^{13} = 3^{22} \cdot 7^5 \cdot 11^{22}$.

Again, we can see – after a bit of thought – that this can't happen: Suppose we had equality. Divide both sides by 7^5. Since 7 still divides the left-hand-side, it must also divide $3^{22} \cdot 11^{22}$. This implies (by Corollary 2.9 again) that $7|3$ or $7|11$, a contradiction.

These ideas can be adapted to show that if one product of primes is equal to another product of primes then the primes occurring in both expressions must be the same, and they must occur the same number of times in each expression; i.e. a natural number can be expressed in one and only one way as a product of prime numbers:

Remark 5.2. *From now on, to keep our statements simple, when we say that a number is expressed as a product of primes, we include the possibility that the product has only one factor; i.e. that it is just a single prime.*

Theorem 5.3 (The Fundamental Theorem of Arithmetic)**.** *Every positive integer greater than* 1 *is equal to a product of prime numbers,* uniquely up to order*.*

To be precise about the uniqueness statement:

If $n > 1$ and $n = p_1 \cdots p_t = q_1 \cdots q_s$ where the $p_1, \dots, p_t, q_1, \dots, q_t$ are all prime numbers and $p_1 \leq p_2 \leq \cdots \leq p_t$ and $q_1 \leq q_2 \leq \cdots \leq q_s$ then $s = t$ and $p_1 = q_1$, $p_2 = q_2$,. . . ,$p_t = q_t$.

Proof. We have already proved that every integer greater than 1 factors as a product of primes. It remains to prove the uniqueness assertion.

We'll use strong induction on $n > 1$. Now $n = 2$ is prime and hence has only the trivial factorization 2.

Suppose the result is known for $2, \dots, n$ and that we have two (possibly the same) factorizations

$$n + 1 = p_1 \cdots p_t = q_1 \cdots q_s, \quad \text{with } p_1 \leq p_2 \leq \cdots \leq p_t,\ q_1 \leq q_2 \leq \cdots \leq q_s$$

Let r be the largest prime number that divides $n + 1$. Then $r | p_1 \cdots p_t \implies r | p_i$ for some i (by Corollary 2.9) and hence $r = p_i$ (since p_i is prime). But then we must have $r = p_t$ since r is the largest prime dividing $n + 1$. An identical argument with the other expression shows $r = q_s$. Thus $p_t = r = q_s$.

It follows (on dividing by r) that

$$\frac{n+1}{r} = p_1 \cdots p_{t-1} = q_1 \cdots q_{s-1}.$$

Since $(n + 1)/r < n + 1$, it follows from our induction hypothesis that $t - 1 = s - 1$ (and hence $t = s$) and that $p_1 = q_1$,. . . , $p_{t-1} = q_{t-1}$. □

The Fundamental Theorem of Arithmetic says that integers greater than 1 factorize *in a unique way* as a product of prime numbers

$$n = p_1 p_2 \cdots p_t \text{ with } p_1 \leq p_2 \leq \cdots \leq p_t.$$

Thus

$$7000 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 5 \cdot 7.$$

We can collect together equal primes and write them as powers. We then get

$$n = q_1^{a_1} \cdots q_r^{a_r} \text{ with } q_1 < \cdots < q_r \text{ and } a_1, \dots, a_r \geq 1.$$

For example,

$$7000 = 2^3 \cdot 5^3 \cdot 7.$$

Notation 5.4. *Given a prime p and a nonzero integer n, we write '$p^a \| n$' to mean that $p^a | n$ but $p^{a+1} \not| n$; i.e. that a is the* exact power *of p which divides n.*

Example 5.5. $2^2 \| 12$, $3^3 \| 108$, $5^4 \| 20000$, *etc*

Recall that $n! := 1 \cdot 2 \cdots (n-1) \cdot n$.

Let $p < n$ be a prime. What is the exact power of p that divides $n!$?

Solution: The number of integers smaller than or equal to n which are divisible by p is $\lfloor n/p \rfloor$.

Of these, some are divisible by p^2 and so contribute an extra factor of p in $n!$. There are $\lfloor n/p^2 \rfloor$ numbers less than or equal to n which are divisible by p^2.

Similarly, there are $\lfloor n/p^3 \rfloor$ numbers less than or equal to n which are divisible by p^3, and each of these contributes yet another factor of p.

Continuing like this (until p^k is too large), the total power of p which divides $n!$ is

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

Example 5.6. *What is the exact power of* 3 *which divides* 20!.

Answer:

$$\left\lfloor \frac{20}{3} \right\rfloor + \left\lfloor \frac{20}{9} \right\rfloor = 6 + 2 = 8.$$

So $3^8 \| 20!$.

Example 5.7. *Factorize* 20! *as a product of prime numbers.*

Solution: *For each prime up to* 19*, we determine the exact power that divides* 20! *(as in the last example):* $2^{18} \| 20!$, $3^8 \| 20!$, $5^4 \| 20!$, $7^2 \| 20!$, $11, 13, 17, 19 \| 20!$. *Thus*

$$20! = 2^{18} \cdot 3^8 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19.$$