

University of Western Australia
DEPARTMENT OF MATHEMATICS

UWA ACADEMY
FOR YOUNG MATHEMATICIANS

Number Theory II

Greg Gamble

Review of Primes

Which numbers are primes? This is really a hard question to answer . . . if I give you a number with lots of digits in it, it might be easy for you to tell me that that number is *not* prime, but if it happens to be prime then it will probably take you a long time to determine this. In fact, there are lots of *unsolved* problems related to primes. Can we get a list of *small-ish* primes? . . . The answer to this question is yes! Below is a fun way of doing this; it was devised by a Greek mathematician named *Eratosthenes* (pronounced: error-toss-the-knees); in his honour the method is called the *Sieve of Eratosthenes*.

⚡ Eratosthenes (c. 276 BC–194 BC) was a Greek mathematician, historian, astronomer, poet and geographer. Born at Cyrene in northern Africa he lived much of his life in Alexandria where he was the chief librarian. (At the time, Alexandria was famous for its library.) Eratosthenes was also famous for estimating the circumference of the earth using elementary *trigonometry* (i.e. *geometry*) and the lengths of shadows in two different places (measured at the same time of day.)

Sieve of Eratosthenes

The *Sieve of Eratosthenes* is a method for finding all the *primes* less than (or equal to) some number N . This is done by performing the following steps.

1. Start by writing down all the *natural numbers* from 1 *upto* N .
2. Cross out 1 . . . 1 is *not* prime (by definition).
3. The first number *not* crossed out is 2 . . . it must be *prime*; put a *box* around it and cross out *all* multiples of 2 in the list . . . i.e. cross out 4, 6, 8,
4. Go back to the start of the list and *box* the first number that is *not* crossed out or boxed . . . it must be *prime*; and cross out *all* multiples of that number in the list. (*Note*. Some multiples may already have been crossed out.)
5. Repeat *Step 4*. until every number in the list is either *boxed* or crossed out.

After performing these steps, the list of *all* primes less than or equal to N are just those numbers that are *boxed*.

Example 1. Let's use the Sieve of Eratosthenes to find all the primes less than or equal to 30. Below is the list of numbers from 1 to 30, after the method has been applied.

| | | | | | | | | | |
|--|---|--|---------------|---|---------------|--|---------------|--|---------------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |

The following are the steps required to obtain this.

1. List natural numbers from 1 upto 30.
2. Cross out 1.
3. The first number not crossed out is 2; box it and cross out 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30 (all multiples of 2 – other than 2 itself – in the list).
4. The first number not crossed out or boxed is now 3; box it and cross out 9, 15, 21, 27 (all multiples of 3 – other than 3 itself – in the list; 6, 12, 18, 24, 30 are also multiples of 3 but have already been crossed out).
5. The first number not crossed out or boxed is now 5; box it and cross out 25 (the only multiple of 5 left that hasn't already been crossed out or boxed; 10, 15, 20, 30 are also multiples of 5 but have already been crossed out).

On further repeats of Step 4. we box 7, 11, 13, 17, 19, 23, 29 ... it turns out that on each of these occasions there are no multiples left to cross out.

So the list of primes less than or equal to 30 is:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

Exercises.

1. Why were there no multiples of 7, 11, 13, 17, 19, 23 and 29 left to cross out in *Step 5.*, “on further repeats of *Step 4.*,” in Example 1?

Solution. The square of each of 7, 11, 13, 17, 23, 29 is greater than 30. So any multiple of 7, for example, that is less than 30, necessarily has a divisor less than 7 (14 has divisor 2, 21 has divisor 3) and so such multiples have already been crossed out.

2. If $n^2 + n + 41$ is evaluated for every integer n in $\{1, 2, 3, 4, \dots, 39\}$ we have a list of primes. Check this for a few values of n . Is $n^2 + n + 41$ prime for every natural number n ?

Solution. No, $n^2 + n + 41$ is *not* prime for every natural number n . Clearly, whenever n is a multiple of 41, we have $41 \mid n^2 + n + 41$. A similar argument shows that no *polynomial* in n with integer coefficients exists that gives a *prime* for each natural number n ... multiples of the constant term of the polynomial will always yield counter-example values for n . The values of $n^2 + n + 41$ for $n \in \{1, 2, 3, 4, \dots, 39\}$ are:

| | | | | | | | | | |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|------|
| 43, | 47, | 53, | 61, | 71, | 83, | 97, | 113, | 131, | 151, |
| 173, | 197, | 223, | 251, | 281, | 313, | 347, | 383, | 421, | 461, |
| 503, | 547, | 593, | 641, | 691, | 743, | 797, | 853, | 911, | 971, |
| 1033, | 1097, | 1163, | 1231, | 1301, | 1373, | 1447, | 1523, | 1601, | |

It is an interesting coincidence that these numbers are all prime.

3. Is the list of prime numbers *finite*? i.e. is there a *largest* prime number? Here is some help in answering the question. The idea is due to Euclid.

- (i) Suppose we can write all the primes down, in order, from smallest to largest.
- (ii) Multiply all these numbers together and add 1. Call this number N .
- (iii) Can any of the primes in your list divide N ?
- (iv) What do you deduce from your answer to (iii)?

Solution.

- (i) We suppose the list of primes is *finite* and let the list of all primes from smallest to largest be

$$2 = p_1, 3 = p_2, p_3, \dots, p_n.$$

- (ii) Let

$$N = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1.$$

- (iii) None of p_1, p_2, \dots, p_n divides N since

$$N \equiv 1 \pmod{p_k}$$

for each prime p_k in the list.

- (iv) So N is either *prime* itself or has a *prime* divisor other than the primes of our list. In either case, our list of primes is incomplete. So there must be a prime bigger than p_n , contradicting our original assumption. Thus the list of *primes* cannot be *finite*.

Transitivity

The *relation =* is said to be *transitive* since, for any x, y, z ,

$$\mathbf{if } x = y \text{ and } y = z \mathbf{ then } x = z.$$

Suppose a, b, c, d, e are abbreviations for some numerical expressions, (e.g. a might be $3 + 4 + 5$ and b might be $3 + 9$ etc.); suppose also that $a = b, b = c, c = d, d = e$. Then from $a = b$ and $b = c$ we can deduce that $a = c$; from $a = c$ and $c = d$ we can deduce $a = d$; and from $a = d$ and $d = e$ we can deduce $a = e$. Each deduction uses the *transitive* property of $=$. If b, c, d, e are relabelled as a_1, a_2, a_3, a_4 you might also see that the proof of $a = a_4$ was done by *mathematical induction*. We normally write down a proof of $a = e$ in the following way:

$$\begin{aligned} a &= b \\ &= c \\ &= d \\ &= e. \end{aligned}$$

Every time you set out a proof this way you are actually using both *induction* and the *transitive* property of $=$. Here is a concrete example for you to fix these ideas on.

$$\begin{aligned}(a - b)(a^2 + ab + b^2) &= a(a^2 + ab + b^2) - b(a^2 + ab + b^2) \\ &= a^3 + a^2b + ab^2 - a^2b - ab^2 - b^3 \\ &= a^3 - b^3.\end{aligned}$$

Generally, mathematicians tend to leave it like that, but what we have proved is that

$$(a - b)(a^2 + ab + b^2) = a^3 - b^3.$$

A number of other relations are *transitive*, e.g. $>$, $<$, \geq , \leq and \equiv (*congruence modulo m for some natural number m*).

Exercises.

4. Find an example to show that \neq is *not* a *transitive* relation.

Solution. $2 \neq 3$ and $3 \neq 2$, but $2 = 2$ (i.e. $2 \neq 2$ is *false*). So \neq is *not transitive*.


Review of Divisibility and Congruence

The following statements are equivalent (i.e. mean the same thing), where m is a natural number and b is an integer.

- m divides b .
- $m \mid b$.
- $b = mq$ for some integer q .
- b is congruent to 0 modulo m .
- $b \equiv 0 \pmod{m}$.

The following statements are equivalent where m is a natural number and b, r are integers.

- m divides $b - r$.
- $m \mid b - r$.
- $b = mq + r$ for some integer q .
- b is congruent to r modulo m .
- $b \equiv r \pmod{m}$.

 r can only be called a *remainder* here, if it satisfies $0 \leq r < m$; in which case, q is called a *quotient*.

Properties of Congruence modulo m

Suppose $m \in \mathbb{N}$ and a, b, c are integers a, b . Then *congruence modulo m* has the following properties.

- if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$ (i.e. *congruence modulo m is transitive.*)
- if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then

$$\begin{aligned}a + c &\equiv b + d \pmod{m} \\ a \cdot c &\equiv b \cdot d \pmod{m}\end{aligned}$$

- if $a \equiv b \pmod{m}$ and n is a natural number then

$$a^n \equiv b^n \pmod{m}.$$

Binomial expansions

You should be familiar with the following binomial expansions:

$$\begin{aligned}(a + b)^2 &= a^2 + 2ab + b^2 \\ (a + b)^3 &= a^3 + 3a^2b + 3ab^2 + b^3.\end{aligned}$$

Replacing b with $-b$ in the above expansions gives:

$$\begin{aligned}(a - b)^2 &= a^2 - 2ab + b^2 \\ (a - b)^3 &= a^3 - 3a^2b + 3ab^2 - b^3.\end{aligned}$$

In general, for a natural number n and any numbers a and b :

$$(a + b)^n = a^n + na^{n-1}b + \dots + \binom{n}{r}a^{n-r}b^r + \dots + nab^{n-1} + b^n,$$

where for each integer r (between 1 and n inclusive)

$$\binom{n}{r} = \frac{n \cdot (n-1) \cdots (n-r+1)}{1 \cdot 2 \cdots r} = \frac{n!}{r!(n-r)!}.$$

The above expansion is known as the **Binomial Theorem** and the number $\binom{n}{r}$ (also written: nC_r) is known as a *binomial coefficient*. The way to think of the *binomial coefficient*

$$\binom{n}{r}$$

is the *numerator* is a product of r consecutive integers *descending* from n , and the *denominator* is a product of r consecutive integers *ascending* from 1. For convenience we define

$$\binom{n}{0} = 1.$$



Mathematicians have a convention that an *empty* product is 1. Incidentally, an *empty* sum is 0.

Binomial coefficients have a number of very interesting properties. For the moment we will only need the following properties, where n is a natural number and r is an integer such that $0 \leq r \leq n$:

- $\binom{n}{r}$ is always a *natural number*;
- if n is prime and $1 \leq r \leq n - 1$ then n divides $\binom{n}{r}$.

Example 2.

(i) The following expansion demonstrates that the binomial coefficients are natural numbers:

$$\begin{aligned} (a + b)^4 &= a^4 + \binom{4}{1}a^3b + \binom{4}{2}a^2b^2 + \binom{4}{3}ab^3 + b^4 \\ &= a^4 + \frac{4}{1}a^3b + \frac{4 \cdot 3}{1 \cdot 2}a^2b^2 + \frac{4 \cdot 3 \cdot 2}{1 \cdot 2 \cdot 3}ab^3 + b^4 \\ &= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4. \end{aligned}$$

(ii) The following expansion demonstrates the second property above:

$$(a + b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5.$$

Observe that each of the coefficients 5, 10, 10 and 5 is divisible by 5.

Fermat's Little Theorem

We met Fermat's Little Theorem in one of the problems last time:

Theorem (Fermat's Little Theorem).¹ If n is a natural number and p is a prime then $p \mid n^p - n$.

One way of proving Fermat's Little Theorem (in general) involves the following steps, where p is a prime and n is a natural number. You shouldn't have too much trouble with the first two steps ... they are left as an exercise. The third step requires induction and that, after all, is what this set of notes is about.

1. Show p divides $\binom{p}{r}$ for $1 \leq r \leq p - 1$.
2. Deduce $(n + 1)^p \equiv n^p + 1 \pmod{p}$.
3. Using 2. and *induction* show $n^p \equiv n \pmod{p}$.

¹Technically what we give as Corollary 1 (or something equivalent to it) is what is generally regarded as Fermat's Little Theorem.

Proof.

- The proposition we are trying to prove is

$$P(n) : n^p \equiv n \pmod{p}.$$

- We show $P(1)$ is true:

Now $1^p = 1$ for any prime p . So

$$1^p \equiv 1 \pmod{p}$$

i.e. $P(1)$ is true.

- Now we perform the *inductive* step. We will do this two ways. The first is the “... ” way.
Inductive Step (first way):

$$\begin{aligned} 2^p &= (1 + 1)^p \\ &\equiv 1^p + 1 \pmod{p} \\ &\equiv 1 + 1 \pmod{p} \\ &\equiv 2 \pmod{p} \end{aligned}$$

$$\begin{aligned} 3^p &= (2 + 1)^p \\ &\equiv 2^p + 1 \pmod{p} \\ &\equiv 2 + 1 \pmod{p} \\ &\equiv 3 \pmod{p} \end{aligned}$$

⋮

$$\begin{aligned} n^p &= (n - 1 + 1)^p \\ &\equiv (n - 1)^p + 1 \pmod{p} \\ &\equiv (n - 1) + 1 \pmod{p} \\ &\equiv n \pmod{p} \end{aligned}$$

Inductive Step (second way): The second way is more formal and abbreviates the first. We show, for a general natural number k ,

if $P(k)$ is true then $P(k + 1)$ is also true.

Hence, we assume $P(k)$ is true, i.e. we assume

$$k^p \equiv k \pmod{p}.$$

Now we wish to deduce that $P(k + 1)$ is true. Now $P(k + 1)$ is of the form LHS = RHS. So to show it is true we start with one side and *reduce* it to the other side:

$$\begin{aligned} (k + 1)^p &\equiv k^p + 1 \pmod{p} \\ &\equiv k + 1 \pmod{p}, \text{ by our assumption that } P(k) \text{ is true.} \end{aligned}$$

So, if $P(k)$ is true then $P(k + 1)$ is true.

Hence, since $P(1)$ is true, $P(n)$ is true for all $n \in \mathbb{N}$.

□

Fermat's Little Theorem has the following (almost immediate) corollaries.

Corollary 1. *If n is a natural number and p is a prime then $p \mid n$ or $p \mid n^{p-1} - 1$.*

Corollary 2. *If n is a natural number and p is a prime then $p \mid n$ or $p \mid n^{\ell(p-1)} - 1$, for any $\ell \in \mathbb{N}$.*

The last statement is equivalent to the following

Corollary 3. *Let k, n be natural numbers and suppose p is a prime. If*

$$k \equiv 1 \pmod{p-1}$$

then

$$p \mid n^k - n.$$

Greatest common divisor

The *greatest common divisor* (or *highest common factor*) of two integers a, b , denoted by $\gcd(a, b)$ or $\text{hcf}(a, b)$ or simply (a, b) , is the largest natural number that divides both a and b . (Here we must insist that a and b are not both zero.)

Example 3.

(i) $(9, 12) = 3$.

(ii) $(25, 9) = 1$.

(iii) $(-49, 14) = 7$.



If $(a, b) = 1$ then a, b are said to be *relatively prime* or *coprime*.

The *greatest common divisor* d of two integers a, b has three interesting properties:

- d also divides $a - bm$ for any integer m ;
- $d = (a - bm, b)$ for any integer m ;
- there are integers x, y such that $d = ax + by$.

These properties are the basis of the *Euclidean algorithm* method for finding the *greatest common divisor* d of two integers a, b , which is demonstrated below.

Example 4. *To find the gcd of 234 and 180, perform the following steps.*

1. Draw 3 parallel vertical lines.
2. Write 234 and 180 in the two internal columns.
3. Divide the smaller number 180 into the larger 234. Write the quotient in the column adjacent to 234, and the remainder below 234.

4. Repeatedly divide back and forth in a similar way to Step 3. until one number divides (evenly) into the other. At this point that number is the gcd.

$$1 \left| \begin{array}{c|c} 234 & 180 \\ \hline 180 & 162 \\ \hline 54 & 18 \end{array} \right| 3$$

Here 180 was divided into 234, it went once remainder 54; then 54 was divided into 180, it went 3 times remainder 18; and 18 divides 54 (so we stop) ... and so 18 is the gcd of 234 and 180.

Working backwards we can also find x, y such that $234x + 180y = 18$:

$$\begin{aligned} 18 &= 180 - 162 \\ &= 180 - 3 \cdot 54 \\ &= 180 - 3(234 - 1 \cdot 180) \\ &= 4 \cdot 180 - 3 \cdot 234. \end{aligned}$$

So $x = 4$ and $y = -3$ is one possibility. All pairs x, y satisfy

$$\begin{aligned} x &= 4 + 180t \\ y &= -3 + 234t \end{aligned}$$

for some integer t .

Least common multiple


The *least common multiple* of two integers a, b , denoted by $\text{lcm}(a, b)$, is the least natural number that is a multiple of both a and b .

Example 5.

(i) $\text{lcm}(9, 12) = 36$.

(ii) $\text{lcm}(25, 9) = 225$.

(iii) $\text{lcm}(-49, 14) = 98$.

 When one calculates $\frac{5}{9} + \frac{7}{12}$, we would usually first find the lcm of 9 and 12; only we would call it the *lowest common denominator*.

An interesting property of the lcm of a, b links it with the gcd of a, b :

$$\text{lcm}(a, b) = \frac{|a \cdot b|}{\text{gcd}(a, b)}.$$

(Here we must insist that a and b are not both zero.)