

University of Western Australia
DEPARTMENT OF MATHEMATICS

UWA ACADEMY
FOR YOUNG MATHEMATICIANS


Number **Theory II**

Greg Gamble

June 7, 1997

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:

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

Congruence modulo m

Suppose $m \in \mathbb{N}$. Then for two integers a, b we say:

$$a \text{ is congruent to } b \text{ modulo } m$$

$$(\text{written: } a \equiv b \pmod{m})$$

if and only if

$$a \text{ and } b \text{ give the same remainder on division by } m,$$

$$(\text{in which case: } m \mid a - b).$$

The reason that \equiv looks so much like $=$, is that it behaves very much like $=$ does between integers. In particular, *congruence modulo m* has the following properties.

- if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.



This property is called *transitivity*.

- if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then

$$a + c \equiv b + d \pmod{m}$$

$$a \cdot c \equiv b \cdot d \pmod{m}$$

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

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

This follows from the previous (multiplication) property, since, if $a \equiv b \pmod{m}$ then

$$a^n \equiv a \cdot a \cdots a \pmod{m}$$

$$\equiv b \cdot b \cdots b \pmod{m}$$

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

⚠ Also like = the problem: $ax \equiv b \pmod{m}$ where a, b are *known* integers and x is the *unknown*, need not have solutions for x .

Example 2.

- (i) $6 \equiv 1 \pmod{5}$ and $11 \equiv 1 \pmod{5}$. So $6 \equiv 11 \pmod{5}$. In fact, the integers n such that $n \equiv 1 \pmod{5}$ are precisely those integers that can be written in the form:

$$5k + 1$$

for some integer k . In fact, if k is an integer then

$$n = 5k \quad \text{if and only if} \quad n \equiv 0 \pmod{5}$$

$$n = 5k + 1 \quad \text{if and only if} \quad n \equiv 1 \pmod{5}$$

$$n = 5k + 2 \quad \text{if and only if} \quad n \equiv 2 \pmod{5}$$

$$n = 5k + 3 \quad \text{if and only if} \quad n \equiv 3 \pmod{5}$$

$$n = 5k + 4 \quad \text{if and only if} \quad n \equiv 4 \pmod{5}$$

- (ii) $7 \equiv 1 \pmod{6}$ and $231 \equiv 3 \pmod{6}$. So

$$7 + 231 \equiv 1 + 3 \pmod{6}$$

$$\equiv 4 \pmod{6}; \text{ and}$$

$$7 \cdot 231 \equiv 1 \cdot 3 \pmod{6}$$

$$\equiv 3 \pmod{6}.$$

We have seen that *addition* and *multiplication modulo m* , behaves just like we might expect. Similarly, *subtraction* is just as one would expect. What about *division*? Here some care is needed:

Lemma 1. If $ac \equiv bc \pmod{m}$ and $(c, m) = 1$ then $a \equiv b \pmod{m}$.

Lemma 2. If $ac \equiv bc \pmod{m}$ and $(c, m) = d$ then $a \equiv b \pmod{m/d}$.

Summary 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 .
- $b \equiv r \pmod{m}$.

Fermat's Little Theorem. If $n \in \mathbb{N}$, p is a prime and $p \nmid n$ then $n^{p-1} \equiv 1 \pmod{p}$.

Proof. Suppose r is an integer such that $0 < r < p$. Then $rn \equiv s \pmod{p}$ for some integer s also satisfying $0 < s < p$ (since $rn \equiv 0 \pmod{p}$ would imply $p \mid n$ contrary to assumption). Furthermore, for distinct values of r we obtain different values of s , since if

$$r_1n \equiv s \pmod{p} \quad \text{and} \quad r_2n \equiv s \pmod{p},$$

then $r_1n \equiv r_2n \pmod{p}$ whence $r_1 = r_2$ by Lemma 1. Hence

$$1n \cdot 2n \cdot 3n \cdots (p-1)n \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

which on cancellation (using Lemma 1) gives

$$n^{p-1} \equiv 1 \pmod{p}.$$

□

Corollary. If $n \in \mathbb{N}$, p is a prime then $n^p \equiv n \pmod{p}$.

Proof. If $p \nmid n$ then the result follows from Fermat's Little Theorem by multiplying both sides of the congruence by n . Otherwise $n \equiv 0 \pmod{p}$, in which case the result is trivially true. □