

UWA ACADEMY  
FOR YOUNG MATHEMATICIANS

More Number Theory &  
An Application to Cryptosystems

Greg Gamble

November 19, 1996

## Review

Recall that Number Theory is principally concerned with properties of the *natural numbers*:

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

and more generally with the *integers*:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

## Divisibility

In the last Number Theory lecture the term *divides* and the symbol:  $\mid$  (divides) were defined. To refresh your memory the following statements all say the same thing about integers  $a, b$  where  $a \neq 0$ .

- $a$  divides  $b$ .
- $a \mid b$ .
- $b = aq$  for some integer  $q$  (such an integer  $q$  is called a *quotient*).
- $b/a$  is an integer.
- $b$  is *divisible* by  $a$ .
- $b$  is a *multiple* of  $a$ .

⚠ Don't confuse the *divides* symbol:  $\mid$  (which is a *vertical* stroke with a little space around it) with the *slash* symbol:  $/$  (which separates the numerator and denominator of a fraction). Also, note that despite the symmetry of the symbol:  $\mid$  the symbol cannot be used in reverse, i.e.  $a \mid b$  and  $b \mid a$  mean *different* things (in fact, if they are *both* true then  $a = \pm b$ ).

**Division Algorithm.** For integers  $a, b$  with  $a \neq 0$  there exist integers  $q$  (the *quotient*) and  $r$  (the *remainder*) such that

$$b = aq + r \text{ and } 0 \leq r < a.$$

Essentially they are the numbers that make the following division work:

$$\begin{array}{r} q \text{ rem. } r \\ a \overline{) b} \end{array}$$

**Property 1.** If  $a \mid b$  and  $a \mid c$  then  $a \mid bm + cn$  for any integers  $m, n$ .

### 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.)

◊ 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 1.** 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

$$\begin{aligned} x &= 4 + 13t \\ y &= -3 - 10t \end{aligned}$$

for some integer  $t$ .

## Prime numbers

A *prime number* is a *natural number* larger than 1 that is only divisible by *itself* and 1.

A *natural number* that is neither 1 nor prime is called *composite*.

⚡ Notice that 1 is neither *prime* nor *composite*. In fact, 1 is called a *unit* (the technical term for a number that divides all integers).

What makes *primes* so interesting is that every *natural number* (other than 1) can be expressed in just one way (except that we may be able to arrange the factors in many ways) as the product of prime divisors, e.g.

$$74844 = 2^2 \cdot 3^5 \cdot 7 \cdot 11.$$

Such a factorisation is called a *prime decomposition*.

⚡ If we were to include 1 as a prime then  $74844 = 1^5 \cdot 2^2 \cdot 3^5 \cdot 7 \cdot 11$ , say, would be “another prime decomposition”. Excluding 1 as a prime ensures the *uniqueness* of *prime decompositions*.

The following useful properties of primes were introduced in the previous Number Theory Lecture.

**Euclid’s Lemma.** *If a prime  $p$  divides  $ab$  then  $p \mid a$  or  $p \mid b$ .*

**Fermat’s Little Theorem.** *If  $p$  is prime and  $p \nmid a$  then  $p \mid a^{p-1} - 1$ .*

## Congruence modulo $m$

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

$a$  is congruent to  $b$  modulo  $m$

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

$\iff$

$a$  and  $b$  give the same *remainder* on division by  $m$ ,


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

Using congruences we have a new way of expressing divisibility. 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 $m$

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


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

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

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

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

$$\begin{aligned} a^n &\equiv a \cdot a \cdots a \pmod{m} \\ &\equiv b \cdot b \cdots b \pmod{m} \\ &\equiv b^n \pmod{m} \end{aligned}$$

 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

$$\begin{aligned} n = 5k &\quad \text{if and only if} \quad n \equiv 0 \pmod{5} \\ n = 5k + 1 &\quad \text{if and only if} \quad n \equiv 1 \pmod{5} \\ n = 5k + 2 &\quad \text{if and only if} \quad n \equiv 2 \pmod{5} \\ n = 5k + 3 &\quad \text{if and only if} \quad n \equiv 3 \pmod{5} \\ n = 5k + 4 &\quad \text{if and only if} \quad n \equiv 4 \pmod{5} \end{aligned}$$

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

$$\begin{aligned}7 + 231 &\equiv 1 + 3 \pmod{6} \\ &\equiv 4 \pmod{6}; \text{ and} \\ 7 \cdot 231 &\equiv 1 \cdot 3 \pmod{6} \\ &\equiv 3 \pmod{6}.\end{aligned}$$

### Re-expression of some previous results

Let's now look at expressing Property 1, Euclid's Lemma and Fermat's Little Theorem in terms of congruences.

**Property 1.** If  $b \equiv 0 \pmod{a}$  and  $c \equiv 0 \pmod{a}$  then

$$bm + cn \equiv 0 \pmod{a}.$$

**Euclid's Lemma.** If  $p$  is prime and  $ab \equiv 0 \pmod{p}$  then


$$a \equiv 0 \pmod{p} \quad \text{or} \quad b \equiv 0 \pmod{p}.$$

**Fermat's Little Theorem.** If  $p$  is prime and  $a \not\equiv 0 \pmod{p}$  then

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

### More about 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 3.** *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.*

<del>1</del>	<span style="border: 1px solid black; padding: 2px;">2</span>	<span style="border: 1px solid black; padding: 2px;">3</span>	<del>4</del>	<span style="border: 1px solid black; padding: 2px;">5</span>	<del>6</del>	<span style="border: 1px solid black; padding: 2px;">7</span>	<del>8</del>	<del>9</del>	<del>10</del>
<span style="border: 1px solid black; padding: 2px;">11</span>	<del>12</del>	<span style="border: 1px solid black; padding: 2px;">13</span>	<del>14</del>	<del>15</del>	<del>16</del>	<span style="border: 1px solid black; padding: 2px;">17</span>	<del>18</del>	<span style="border: 1px solid black; padding: 2px;">19</span>	<del>20</del>
<del>21</del>	<del>22</del>	<span style="border: 1px solid black; padding: 2px;">23</span>	<del>24</del>	<del>25</del>	<del>26</del>	<del>27</del>	<del>28</del>	<span style="border: 1px solid black; padding: 2px;">29</span>	<del>30</del>

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 3?

**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. 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*.

Above we observed that:

**Theorem.** If  $n > 1$  and  $n$  has no divisors less than  $\sqrt{n}$  then  $n$  is prime.

**Example 4.**

- (i) 97 is prime, since

- 2, 3, 5, 7 are the primes less than 10;
- $97 < 100$  and  $100 = 10^2$  (we don't need to find square-roots exactly!); and
- none of 2, 3, 5, 7 divides 97.

- (ii) The primes less than 100 are:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

This is easy to check, because at most we need only check divisibility by 2, 3, 5 and 7. Incidentally, there are 25 of them!

## Cryptosystems


A *cryptosystem* is an algorithm used to encode a message to keep it *secret*. To describe some of these it will be useful to start with a numerical encoding of the alphabet and the blank space between words:

letter	space	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
encoding	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

One of the simplest codes (cryptosystems) is the *Caesar cipher* which replaces each letter (with encoding  $n$ ) of a message by the letter with encoding  $r$ , where:

$$r \equiv an + b \pmod{q}$$

where  $a, b, q$  are fixed integers such that  $a$  and  $q$  are coprime and  $q$  is at least as large as the number of letters in your alphabet. For our alphabet above we would need  $q$  to be at least 27.

 The cipher is named for Julius Caesar who used such a code with  $a = 1$  and  $b = 3$ . If we choose  $q = 27$  with Julius Caesar's choice for  $a$  and  $b$  encoding a message amounts to a *cyclic shift* of each letter right by 3 letters. This simple example is easy to break ... by determining the encoding of just one letter of the message, by trial-and-error (there are only 27 possibilities to check ... and by picking on the most frequently occurring letter of the encoded message we might try 'e' first, etc.).


Another simple code is the *one-time pad*. The way this works is that both the receiver and sender have a long sequence of random numbers,  $(m_1, m_2, \dots)$ . If a message with the simple numerical encoding of the letters is:

$$n_1, n_2, \dots, n_i, \dots$$

then the  $i^{\text{th}}$  letter of the encoded message is encoded as

$$n_i + m_i \pmod{q},$$

where  $q$  may be 27 if spaces are encoded or 26 if they are not encoded. Each sequence of random numbers is used just *once* which makes the code *unbreakable*. The method is however extremely cumbersome, because both sender and receiver must keep a very long sequence of numbers.

 A one-time pad is used for the hot-line between Washington and Moscow.

For frequent computer-based communication among several parties it is desirable to have a cryptosystem with neither of the faults of the above systems, i.e.

- (i) the *encoding* and *decoding* algorithms are easy to compute and reusable; and
- (ii) each person's *decoding* algorithm cannot be obtained from his/her *encoding* algorithm in any reasonable amount of time.

The second property means that the *encoding* algorithm can in fact be made public, and so such a system is called a *public-key system*.

## The RSA Cryptosystem

The RSA system is an example of a *public-key system* that was developed in 1977 by Rivest, Shamir and Adleman. It is based on two simple Number Theory results – one you have already seen: Fermat’s Little Theorem – and the following:

**Lemma.** *If  $p$  is prime,  $p \nmid c$  and  $ac \equiv bc \pmod{p}$  then*

$$a \equiv c \pmod{p}.$$

Using these two simple results we get a result that is the basis of the RSA Cryptosystem:

**RSA Theorem.** *Let  $p, q$  be distinct primes;*

$$\begin{aligned} & \text{let } n = pq, \\ & \text{let } k = (p - 1)(q - 1), \\ & \text{choose } d \text{ coprime to } k, \text{ and} \\ & \text{choose } e \text{ such that } de \equiv 1 \pmod{k}. \end{aligned}$$


*Then  $a^{ed} \equiv a \pmod{n}$  for any integer  $a$ .*

Here is an example to show how we use this result to come up with a *cryptosystem*.

**Example 5.** *Suppose our message is ‘GO WEST’. Then we perform the following steps.*

1. *Encode the letters numerically, e.g. by the encoding given in the table on page 8. This gives: 07150023051920. Call this number  $a$ .*
2. *We need  $p, q$  such that  $n = pq > a$ .*
3. *To encode the message, compute:  $a^e \pmod{n}$ .*
4. *To decode the message, the receiver computes:  $(a^e)^d \pmod{n}$ , which by the RSA Theorem is congruent to  $a \pmod{n}$ , and since  $n > a$  we know the message was  $a$ .*

Observe that in our example the message  $a$  was a rather large number and that  $n$  needed to be even larger. In practice  $p$  and  $q$  are large primes (of the order of a 100 digits each). Observe that choosing appropriate  $p, q, d$  determines  $n, k, e$ . The numbers  $e$  and  $n$  for the cryptosystem are publicly announced. The system is secure since determining the decoding algorithm is at least as difficult as factoring  $n$ .

 The technology of 1990 would have required approximately 4 million years on average to factor any 200 digit number that is the product of two equal length primes.

Very long messages may still give a number larger than the simple encoding  $a$ , in which case one needs to break up the message into modules and encode each module separately. Here is one of Rivest, Shamir and Adleman’s own examples.

**Example 6.** Take the message: “IT’S ALL GREEK TO ME” and suppose  $n = 2773$ ,  $d = 157$  and  $e = 17$ . Since we can only encode numbers less than 2773, we choose blocks of length 2.

1. Numerical encoding of the blocks gives (where # denotes a blank space and other punctuation is ignored):

I	T	S	#	A	L	L	#	G	R
09	20	19	00	01	12	12	00	07	18
E	E	K	#	T	O	#	M	E	#
05	05	11	00	20	15	00	13	05	00

2. Observe each block is encoded with a number less than 2773.
3. Encoding the first block we have:  $920^e = 920^{17} \equiv 948 \pmod{2773}$ . Encoding all the blocks we get the following coded form of the message:

09	48	23	42	10	84	14	44	26	63
23	93	07	78	07	74	02	19	16	55

4. The receiver would now decode the message by applying the decoding algorithm to each block, e.g. for the first block

$$948^d = 948^{157} \equiv 920 \pmod{2773}$$

which is the numerical encoding for the first original block: ‘IT’.