

UWA ACADEMY  
FOR YOUNG MATHEMATICIANS

More Number Theory &  
An Application to Cryptosystems:  
Problems with some Solutions

Greg Gamble

1. Prove Fermat's Little Theorem for  $p = 2, 3$  and  $5$  using congruences.

**Solution.**

- For any integer  $a$ ,  $a$  is congruent to either  $0$  or  $1$  modulo  $2$ . So, (noting that  $a^{2-1}$  is just  $a$ ) ...  
if  $a \not\equiv 0 \pmod{2}$  then  $a^{2-1} \equiv 1 \pmod{2}$ .
- Modulo  $3$ ,  $a$  not congruent to  $0$  implies  $a$  is congruent to either  $1$  or  $2$ , whence either  $a - 1$  or  $a + 1$  is congruent to  $0$ . Thus, if  $a \not\equiv 0 \pmod{3}$  then

$$\begin{aligned}a^2 - 1 &= (a - 1)(a + 1) \equiv 0 \pmod{3} \\ &\text{i.e. } a^{3-1} \equiv 1 \pmod{3}.\end{aligned}$$

- Modulo  $5$ ,  $a$  not congruent to  $0$  implies  $a$  is congruent to one of  $-2, -1, 1$  or  $2$ , whence one of  $a + 2, a + 1, a - 1$  or  $a - 2$  is congruent to  $0$ . Thus, if  $a \not\equiv 0 \pmod{5}$  then

$$\begin{aligned}0 &\equiv (a + 1)(a - 1)(a + 2)(a - 2) \pmod{5} \\ &\equiv (a^2 - 1)(a^2 - 4) \pmod{5} \\ &\equiv (a^2 - 1)(a^2 + 1) \pmod{5} \\ &\equiv a^4 - 1 \pmod{5}\end{aligned}$$

$$\text{i.e. } a^{5-1} \equiv 1 \pmod{5}.$$

So Fermat's Little Theorem is true for  $p = 2, 3$  and  $5$ .

2. Show Euclid's Lemma is false if  $p$  is *not* prime.

**Solution.** Removing the condition that  $p$  be prime in Euclid's Lemma, gives the statement:

If  $p \mid ab$  then  $p \mid a$  or  $p \mid b$ .

To show this statement is false, we need only exhibit one counterexample, e.g.

Take  $p = 4, a = 2, b = 6$ . Then  $4 \mid 12 = 2 \cdot 6$ , but  $4 \nmid 2$  and  $4 \nmid 6$ .

So Euclid's Lemma is false if the condition that  $p$  be prime is removed.

3. For which  $a$  does the congruence  $ax \equiv 1 \pmod{m}$  have a solution, when ...

- (i)  $m = 4$ ?                      (ii)  $m = 5$ ?                      (iii)  $m = 6$ ?                      (iv)  $m = 7$ ?

**Solution.** The congruence  $ax \equiv 1 \pmod{m}$  is equivalent to saying that

$$ax + my = 1 \tag{1}$$

for some integer  $y$ . In Problem 16 of the Number Theory I Problem Sheet, we showed that if such a condition was satisfied then  $a, m$  are coprime. Conversely, the Euclidean Algorithm guarantees a solution of (1). Thus, in each case the problem is equivalent to finding integers  $a$  that are coprime with  $m$ . Note that, if  $(a_1, m) = 1$  and  $0 < a_1 < m$  then any  $a \equiv a_1 \pmod{m}$  also satisfies  $(a, m)$ . So we will only list below those  $a$  that are coprime with  $m$  and satisfy  $0 < a < m$ . (Observe  $a$  cannot be 0, since  $(0, m) = m$ .)

⚡ The significance of an  $x$  satisfying  $ax \equiv 1 \pmod{m}$  for some  $a, m$  is that it is a *multiplicative inverse* of  $a$  modulo  $m$  (i.e. it behaves analogously to the *reciprocal* of a non-zero rational number – the *reciprocal*  $1/b$  of a non-zero rational number  $b$  satisfies  $b \cdot (1/b) = 1$ .)

- (i) For  $m = 4$ , if  $a \in \{1, 3\}$  then  $a, m$  are coprime. (If  $a = 1$  (respectively  $a = 3$ ) then  $x = 1$  (respectively  $x = 3$ ) is a solution of  $ax \equiv 1 \pmod{4}$ .)
- (ii) Since  $m = 5$  is prime, for  $a \in \{1, 2, 3, 4\}$  we have  $a, m$  are coprime. (Possibilities for  $x$  are 1, 3, 2, 4 respectively. For each  $a$  there are an infinite number of possibilities for  $x$  but all the possibilities are congruent modulo  $m$ .)
- (iii) For  $m = 6$ , if  $a \in \{1, 5\}$  then  $a, m$  are coprime. (Possibilities for  $x$  are 1, 5 respectively.)
- (iv) Since  $m = 7$  is prime, for  $a \in \{1, 2, 3, 4, 5, 6\}$  we have  $a, m$  are coprime. (Possibilities for  $x$  are 1, 4, 5, 2, 3, 6 respectively.)

4. Solve  $58x \equiv 1 \pmod{127}$ .

[Hint. Use the Euclidean Algorithm as one of your steps.]

**Solution.** Observe that  $58x \equiv 1 \pmod{127}$  is equivalent to saying that

$$58x + 127y = 1 \tag{2}$$

for some integer  $y$ , i.e. a solution exists if and only if 58 and 127 are coprime (see discussion in previous question solution). Thus using the *Euclidean Algorithm*:

$$\begin{array}{r|l} 5 & \begin{array}{l|l} 58 & 127 \\ \hline 55 & 116 \\ \hline 3 & 11 \\ & 12 \\ & \hline & -1 \end{array} & \begin{array}{l} 2 \\ \\ 4 \end{array} \end{array}$$

Thus

$$\begin{aligned} -1 &= 11 - 4 \cdot 3 \\ &= 11 - 4 \cdot (58 - 5 \cdot 11) \\ &= 21 \cdot 11 - 4 \cdot 58 \\ &= 21 \cdot (127 - 2 \cdot 58) - 4 \cdot 58 \\ &= 21 \cdot 127 - 46 \cdot 58 \end{aligned}$$

$$\text{So ... } 1 = -21 \cdot 127 + 46 \cdot 58$$

Hence, by the Theorem of the notes, (2) has general solution

$$\begin{aligned}x &= 46 + 127t \\y &= -21 - 58t\end{aligned}$$

i.e.  $x \equiv 46 \pmod{127}$ .

5. Show  $7 \mid 2222^{5555} + 5555^{2222}$ .

**Solution.** By Fermat's Little Theorem, with  $p = 7$  we have:

If  $n$  is a natural number and  $n \not\equiv 0 \pmod{7}$  then  $n^6 \equiv 1 \pmod{7}$ .

So for natural numbers  $n$ ,  $q$  and  $r$ , if  $n \not\equiv 0 \pmod{7}$  then

$$\begin{aligned}n^{6q+r} &\equiv (n^6)^q \cdot n^r \pmod{7} \\&\equiv 1^q \cdot n^r \pmod{7} \\&\equiv n^r \pmod{7}.\end{aligned}$$

In other words, if  $n \not\equiv 0 \pmod{7}$  then we can reduce the power of  $n$  modulo 6. We use this twice in the second line of our reduction below.

$$\begin{aligned}2222^{5555} + 5555^{2222} &\equiv 3^{5555} + (-3)^{2222} \pmod{7} \\&\equiv 3^5 + (-3)^2 \pmod{7} && \text{since } \pm 3 \not\equiv 0 \pmod{7} \\&\equiv 3^2(3^3 + 1) \pmod{7} \\&\equiv 3^2 \cdot 28 \pmod{7} \\&\equiv 0 \pmod{7}.\end{aligned}$$

Hence  $7 \mid 2222^{5555} + 5555^{2222}$ .

6. 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  $n \dots$  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:

$$\begin{array}{cccccccccccc}43, & 47, & 53, & 61, & 71, & 83, & 97, & 113, & 131, & 151, \\173, & 197, & 223, & 251, & 281, & 313, & 347, & 383, & 421, & 461, \\503, & 547, & 593, & 641, & 691, & 743, & 797, & 853, & 911, & 971, \\1033, & 1097, & 1163, & 1231, & 1301, & 1373, & 1447, & 1523, & 1601.\end{array}$$

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

7. Is 167 prime?

**Solution.** Suppose 167 is composite. Then it has a divisor  $m > 1$ . Then  $m$  and  $167/m$  both divide 167. The lesser of  $m$  and  $167/m$  is at most  $\sqrt{167}$  and must have a prime decomposition consisting of primes less than or equal to  $\sqrt{167}$ . Now  $\sqrt{167} < 13$  and it is easy to check that none of the primes 2, 3, 5, 7 or 11 divide 167. So we have a contradiction. That is, 167 cannot be composite; and since it is not 1 it must be prime.

8. Obtain a complete list of primes less than 1000.

[*Hint.* There are 168 of them!]

**Answer.** Using the *Sieve of Eratosthenes*, the primes less than 1000 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, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, and 997.

If you avoided this problem because you thought it would take too long, note that  $32^2 > 1000$ ; so . . . once you have boxed 31 (the 11<sup>th</sup> prime) all remaining numbers not crossed out must be prime. (So you only need to run through the algorithm 11 times.)

9. Find the values of  $p, q, k$  for Example 6.

**Solution.** From the RSA Theorem we know that  $n, p, q, k, d, e$  satisfy

$p, q$  are distinct primes,

$$n = pq,$$

$$k = (p - 1)(q - 1),$$

$$(d, k) = 1 \text{ and}$$

$$de \equiv 1 \pmod{k}.$$

In particular,

$$\begin{aligned} k &= (p - 1)(q - 1) \\ &= pq - p - q + 1 \\ &= n - (p + q) + 1. \end{aligned}$$

Without loss of generality, assume  $p < q$ . Then  $2 \leq p < \sqrt{n}$  and so  $n/2 - 1 \leq k < n - 2\sqrt{n} + 1$ .

Also the possibilities for  $de$  are:  $1, k + 1, 2k + 1, \dots$ . Since  $de = 157.17 = 2669$  is both greater than  $n/2 - 1$  and less than  $n$  we see that the only possibility is:  $de = k + 1$ . So  $k = de - 1 = 2668$ . Thus:

$$\begin{aligned} p + q &= n - k + 1 \\ &= 2773 - 2668 + 1 = 106. \end{aligned}$$

So we have:

$$\begin{aligned} p + q &= 106 \\ pq &= 2773. \end{aligned}$$

Observe that

$$(x - p)(x - q) = x^2 - (p + q)x + pq,$$

and so  $p, q$  are the solutions of the following quadratic equation

$$x^2 - 106x + 2773 = 0$$

i.e.

$$\begin{aligned} p, q &= \frac{106 \pm \sqrt{106^2 - 4 \cdot 1 \cdot 2773}}{2} \\ &= 53 \pm \sqrt{53^2 - 2773} \\ &= 53 \pm 6 \\ &= 47, 59. \end{aligned}$$

So  $p = 47, q = 59, k = 2668$ . (Remember, we assumed  $p < q$ . Of course,  $p = 59, q = 47$  would also have been a correct solution.)

10. Use  $e = 3$  and  $n = 2773$  to encode the messages using the RSA cryptosystem:

- (i) CODING IS EASY
- (ii) THE HUNS ARE COMING

Use 2-letter blocks and don't omit spaces.

**Solution.**

- (i) • First we numerically encode the letters of the message as per the table on page 8 of the notes:

C	O	D	I	N	G	#	I	S	#	E	A	S	Y
03	15	04	09	14	07	00	09	19	00	05	01	19	25

- Now we encode each block  $a$  with  $b$  according to the algorithm:  $b = a^e \pmod n$ . This gives us the encoding:

1392	2473	1336	0729	1138	1497	1919
------	------	------	------	------	------	------

As an example, the first block of the encoding was obtained as follows

$$\begin{aligned} 315^3 &= 315^2 \cdot 315 = 99225 \cdot 315 \\ &\equiv 2173 \cdot 315 \pmod{2773} \\ &\equiv 1392 \pmod{2773} \end{aligned}$$

Thus the RSA encoding of the message is: 1392247313360729113814971919.

- (ii) • First we numerically encode the letters of the message as per the table on page 8 of the notes:

T	H	E	#	H	U	N	S	#	A	R	E	#	C	O	M	I	N	G	#
20	08	05	00	08	21	14	19	00	01	18	05	00	03	15	13	09	14	07	00

- Now we encode each block  $a$  with  $b$  according to the algorithm:  $b = a^e \pmod n$ . This gives us the encoding:

0952	1479	2235	2092	0001	0749	0027	2421	0848	2084
------	------	------	------	------	------	------	------	------	------

As an example, the first block of the encoding was obtained as follows

$$\begin{aligned} 2008^3 &= 2008^2 \cdot 2008 = 4032064 \cdot 2008 \\ &\equiv 122 \cdot 2008 \pmod{2773} \\ &\equiv 952 \pmod{2773} \end{aligned}$$

Thus the RSA encoding of the message is: 0952147922352092000107490027242108482084.

11. Find the decoding algorithm for the previous exercise.

**Solution.** Let us suppose we don't have available to us the results of Problem 8 of the non-homework set. From the RSA theorem we know that  $n = pq$ , where  $p, q$  are distinct primes. Without loss of generality, take  $p < q$ . Then  $p < \sqrt{2773} < 53$ . So we need to check  $n = 2773$  for divisibility by each of 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, and 47 (there's no shorter way); except that, of course, you might guess that  $p, q$  must surely be "close" to  $\sqrt{2773}$  and thus find  $p = 47$  and  $q = 59$  straight away. Hence, the parameter  $k$  of the RSA Theorem is:

$$k = (p - 1)(q - 1) = 46 \cdot 58 = 2668.$$

Now, the parameter  $d$  satisfies:  $de \equiv 1 \pmod{k}$ . Using the method of Problem 5, we apply the *Euclidean Algorithm* to  $e = 3$  and  $k = 2668$ .

$$\begin{array}{r|l} 3 & 2668 \\ & 2667 \\ \hline & 1 \end{array} \quad 889$$

Thus

$$\begin{aligned} 1 &= 2668 - 889 \cdot 3 \\ &\equiv -889 \cdot 3 \pmod{2668} \\ &\equiv 1779 \cdot 3 \pmod{2668} \end{aligned}$$

So we may take  $d = 1779$ , i.e. the *decoding algorithm* is:  $a = b^{1779} \pmod{2773}$ , where  $b$  is a 4-digit block of the encoded message and  $a$  is the corresponding decoded block, which we recognise as a pair of two-digit numbers which in turn represent letters according to the table on page 8 of the notes.

⚡ Now, 1779 is quite large, so  $b^{1779}$  is well-nigh impossible to work out. This seems to suggest that the *decoding algorithm* is impractical ... but remember we are working *modulo* 2773. Observing that

$$11011110011$$

is the *binary* (i.e. *base two*) representation of 1779, write

$$b^{1779} = b \cdot b^2 \cdot b^{32} \cdot b^{64} \cdot b^{128} \cdot b^{256} \cdot b^{1024} \cdot b^{2048}$$

where

$$\begin{aligned} b^{32} &= (((b^2)^2)^2)^2 \\ b^{64} &= (b^{32})^2 \\ b^{128} &= (b^{64})^2 \\ b^{256} &= (b^{128})^2 \\ b^{1024} &= ((b^{256})^2)^2 \\ b^{2048} &= (b^{1024})^2 \end{aligned}$$

Each time we square or calculate a product we reduce *modulo* 2773. We need to perform 12 squaring operations and 7 product operations to calculate  $b^{1779}$  for any  $b$ . We can write a computer program to do this in the twinkle of an eye and what's more no intermediate calculation involves a number of greater than 7 digits.