

UWA ACADEMY  
FOR YOUNG MATHEMATICIANS

Number Theory III: Problems with Solutions

Greg Gamble

1. 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.)

2. 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  $7 \mid 2222^{5555} + 5555^{2222}$ .

3. 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.

4. 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.)

5. 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*:

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

Thus

$$\begin{aligned} -1 &= 11 - 4.3 \\ &= 11 - 4.(58 - 5.11) \\ &= 21.11 - 4.58 \\ &= 21.(127 - 2.58) - 4.58 \\ &= 21.127 - 46.58 \end{aligned}$$

$$\text{So } \dots \quad 1 = -21.127 + 46.58$$

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

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

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

6. Using the *Caesar cipher*, with  $a, b, m$  as defined in the dangerous bend on page 2 of the notes, encode: CRYPTOLOGY.

**Answer.** With  $a = 1$ ,  $b = 3$  and  $m = 27$ , the *Caesar cipher* amounts to being a cyclic shift of each letter by three letters. Hence CRYPTOLOGY is encoded as:

FUASWRORJA

- \*7. Decode the following message. Spaces are also encoded. There is one space in the encoded output.

RUOELTWK EINHxFEQHZEYTDJPEHVONERUOEBGCAEMHS

(See additional comments and hint in first homework problem.)

**Solution.** First observe that the letters occurring in the message have the following frequencies:

E: 8;            H: 4;            O: 3;            N, R, T, U: 2;  
#, A, B, C, D, F, G, I, J, K, L, M, P, Q, S, V, W, X, Y, Z: 1;

where # represents a  $\langle \text{SPACE} \rangle$ . Since E also occurs in the message every 4–5 letters or so we can be fairly confident that E encodes a  $\langle \text{SPACE} \rangle$ . Then RUO is a three letter word that occurs twice and in particular it comes at the beginning of the message. More than likely RUO encodes THE. Also we are given that a *Caesar cipher* has been used where each letter with numeric encoding  $u$  is encoded as the letter with numeric encoding  $v$  according to

$$v \equiv au + b \pmod{27},$$

for some  $a, b$  such that  $(a, 27) = 1$ . Since  $(a, 27) = 1$ , there exists an integer  $c$  such that  $ca \equiv 1 \pmod{27}$  (see the solutions of questions 4. and 5.), and for such a choice of  $c$  we have

$$\begin{aligned} cv &\equiv cau + cb \pmod{27} \\ u &\equiv cv - cb \pmod{27} && \text{rearranging and using } ca \equiv 1 \pmod{27} \\ u &\equiv cv + d \pmod{27} \end{aligned}$$

where  $d = -cb$ . This is the decoding rule. Now we use our guesses (beside each letter is its corresponding numeric encoding):

# ↔ 0	encodes as	E ↔ 5
T ↔ 20	encodes as	R ↔ 18
H ↔ 8	encodes as	U ↔ 21
E ↔ 5	encodes as	O ↔ 15

The first two of our guesses give:

$$0 \equiv c \cdot 5 + d \pmod{27} \quad (3)$$

$$20 \equiv c \cdot 18 + d \pmod{27} \quad (4)$$

Subtracting (3) from (4) (to eliminate  $d$ ) we obtain:

$$20 \equiv c \cdot 13 \pmod{27} \quad (5)$$

Observe that  $13 \cdot 2 = 26 \equiv -1 \pmod{27}$ . So multiplying (5) throughout by 2 we obtain:

$$40 \equiv 26 \cdot c \pmod{27}$$

$$13 \equiv -1 \cdot c \pmod{27}$$

$$\text{So } \dots \quad c \equiv 14 \pmod{27}$$

Substituting  $c \equiv 14 \pmod{27}$  in (3) gives:

$$d \equiv -14 \cdot 5 \equiv 13 \cdot 5 \pmod{27}$$

$$\equiv 65 \pmod{27}$$

$$\equiv 11 \pmod{27}$$

So our *decoding* algorithm is:

$$u \equiv 14v + 11 \pmod{27}$$

By the way, multiplying the *decoding* algorithm by 2 and rearranging gives the *encoding* algorithm:

$$v \equiv 2u + 5 \pmod{27}$$

Using the *decoding* algorithm we obtain the following *decoding* table:

	# ↔ 0	A ↔ 1	B ↔ 2	C ↔ 3	D ↔ 4	E ↔ 5	F ↔ 6	G ↔ 7	H ↔ 8
decodes as	K ↔ 11	Y ↔ 25	L ↔ 12	Z ↔ 26	M ↔ 13	# ↔ 0	N ↔ 14	A ↔ 1	O ↔ 15
	I ↔ 9	J ↔ 10	K ↔ 11	L ↔ 12	M ↔ 13	N ↔ 14	O ↔ 15	P ↔ 16	Q ↔ 17
decodes as	B ↔ 2	P ↔ 16	C ↔ 3	Q ↔ 17	D ↔ 4	R ↔ 18	E ↔ 5	S ↔ 19	F ↔ 6
	R ↔ 18	S ↔ 19	T ↔ 20	U ↔ 21	V ↔ 22	W ↔ 23	X ↔ 24	Y ↔ 25	Z ↔ 26
decodes as	T ↔ 20	G ↔ 7	U ↔ 21	H ↔ 8	V ↔ 22	I ↔ 9	W ↔ 23	J ↔ 10	X ↔ 24

Observe that the *decoding* table does agree with the two guesses we did not use for working it out. (So things are looking good.) Using the table, we get that the message decodes as:

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

and since this is a perfectly sensible English sentence it would seem we have cracked the code.

8. Find the values of  $p, q, k$  for Example 2 ( $n = 2773, d = 157$  and  $e = 17$ ).

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

$$\begin{aligned} p, q &\text{ are distinct primes,} \\ n &= pq, \\ k &= (p-1)(q-1), \\ (d, k) &= 1 \text{ and} \\ de &\equiv 1 \pmod{k}. \end{aligned}$$

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  $de = 157 \cdot 17 = 2669$  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.)

9. Use  $e = 3$  and  $n = 2773$  to encode the following message using the RSA cryptosystem:

CODING IS EASY

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

**Solution.**

- First we numerically encode the letters of the message as per the table on page 1 of the Number Theory III 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.

**Homework exercises.**

- \*1. Decode the following message. Spaces are also encoded. (It just so happens that no spaces appear after the encoding.)

BKDAKUNFKDWTDBJKNWKFNANTTNLKWNTKKBKIDS  
CKMCCUKYCMFCTJDYKDUJKBKHNSCKFNJDY

Note that a *Caesar cipher* has been used (i.e.  $\langle \text{SPACE} \rangle, A, \dots, Z$  are encoded as 00, 01,  $\dots$ , 26 (as per the table on page 1 of the notes), the *Caesar cipher* algorithm

$$v \equiv au + b \pmod{27}$$

has been applied for each letter  $u$  of the message for some  $a, b$  (which you essentially have to find), and the encoded letter  $v$  has been changed back to a letter using the table on page 1 of the notes again.)

*Note:* Letters and spaces occurring in English text, arranged approximately in order of highest frequency to lowest frequency are

$\langle \text{SPACE} \rangle, E, T, A, I, O, N, S, H, R, D, L, U, \dots$

Also, use the fact that inter-word spaces occur on average every 4–5 letters and use what you know about the possibilities of letters in short words of 1, 2 or 3 letters.

If this problem seems too hard, try doing it without using the fact that a *Caesar cipher* has been used.

*Hint.* Since you want to *decode* you really want to express  $u$  in terms of  $v$ , i.e. you really want to find a  $c, d$  such that

$$u \equiv cv + d \pmod{27}.$$

**Solution.** First observe that the letters occurring in the message have the following frequencies:

K:	14;	N:	8;	D:	7;	C:	6;	T:	5;
F,B,J:	4;	U,Y,W:	3;	M,A,S:	2;	H,L,I:	1.		

Since K is the most frequent letter of the encoded message and it also occurs in the message every 4–5 letters or so we can be fairly confident that K encodes a  $\langle \text{SPACE} \rangle$ . Under this assumption, the message starts with a 1-letter word, followed by a 2-letter word. So we guess that B either represents A or I. If B decodes as A, then we are left with only strange possibilities for the following 2-letter word; so it is more likely that B decodes as I.

Now let's try to work out which letter decodes as E. In the encoded message we find N and D are the next most frequently occurring letters (after K), but both of these occur at the beginning of a 2-letter word – so it would seem unlikely that either of these letters decodes as E. The next most frequently occurring letter in the encoded message is C – it occurs doubled in one word and at the end of several others; so there is a pretty good chance that C decodes as E.

Our guesses are as follows (beside each letter is its corresponding numeric encoding, as per the table on page 1 of the notes):

# $\leftrightarrow$ 0	encodes as	K $\leftrightarrow$ 11
I $\leftrightarrow$ 9	encodes as	B $\leftrightarrow$ 2
E $\leftrightarrow$ 5	encodes as	C $\leftrightarrow$ 3

from which we obtain the following congruences:

$$0 \equiv c.11 + d \pmod{27} \tag{6}$$

$$9 \equiv c.2 + d \pmod{27} \tag{7}$$

$$5 \equiv c.3 + d \pmod{27} \tag{8}$$

Subtracting (7) from (5) (to eliminate  $d$ ) we obtain:


$$c \equiv -4 \equiv 23 \pmod{27} \tag{9}$$

Substituting (9) back in (7) and rearranging we obtain



$$d \equiv 9 - (-4.2) \equiv 17 \pmod{27}$$

So our *decoding* algorithm is:

$$u \equiv -4v + 17 \pmod{27}$$

 Multiplying the *decoding* algorithm by  $-7$  and rearranging gives the *encoding* algorithm:

$$v \equiv -7u + 11 \pmod{27}$$

  Observe that we did not use (6) at all. If we had subtracted (7) from (6) we would have obtained:

$$-9 \equiv 9c \pmod{27}$$

whence by Lemma 2 of the notes,

$$-1 \equiv c \pmod{3},$$

giving us several possibilities for  $c \pmod{27}$ , namely:  $c \equiv 2, 5, 8, 11, 14, 17, 20, 23, 26 \pmod{27}$ .

Using the *decoding* algorithm we obtain the following *decoding* table:

	# ↔ 0	A ↔ 1	B ↔ 2	C ↔ 3	D ↔ 4	E ↔ 5	F ↔ 6	G ↔ 7	H ↔ 8
decodes as	Q ↔ 17	M ↔ 13	I ↔ 9	E ↔ 5	A ↔ 1	X ↔ 24	T ↔ 20	P ↔ 16	L ↔ 12
	I ↔ 9	J ↔ 10	K ↔ 11	L ↔ 12	M ↔ 13	N ↔ 14	O ↔ 15	P ↔ 16	Q ↔ 17
decodes as	H ↔ 8	D ↔ 4	# ↔ 0	W ↔ 23	S ↔ 19	O ↔ 15	K ↔ 11	G ↔ 7	C ↔ 3
	R ↔ 18	S ↔ 19	T ↔ 20	U ↔ 21	V ↔ 22	W ↔ 23	X ↔ 24	Y ↔ 25	Z ↔ 26
decodes as	Z ↔ 26	V ↔ 22	R ↔ 18	N ↔ 14	J ↔ 10	F ↔ 6	B ↔ 2	Y ↔ 25	U ↔ 21

Observe that the *decoding* table does agree with our other guess (K encodes #) that we did not use for working it out. (So things are looking good.) Using the table, we get that the message decodes as:

I AM NOT AFRAID OF TOMORROW FOR I HAVE SEEN YESTERDAY AND  
I LOVE TODAY

and since this is a perfectly sensible English sentence we can be fairly confident that we have cracked the code.

2. Use  $e = 3$  and  $n = 2773$  to encode the following message using the RSA cryptosystem:

THE HUNS ARE COMING

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

**Solution.**

- First we numerically encode the letters of the message as per the table on page 1 of the Number Theory III 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.

\*3. Find the decoding algorithm for the previous problem.

**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 1 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.