Notes on the RSA Algorithm and HW #10

These notes concern the "RSA," or Rivest-Shamir-Adelman, algorithm, which is a method for encoding and decoding messages using some number theory ideas.

The Exercises at the ends of Parts A, B, and C of these Notes constitute HW #10. Anything after the Exercises for Part C can be ignored for the purposes of HW #10, but will be very relevant to subsequent assignments.

Throughout, by "prime," or "prime number," we will mean a *positive* integer p whose only positive integer factors are 1 and p.

The RSA algorithm is based upon the simple idea that, while multiplying together two large primes is relatively easy, *factoring* such a product is much harder.

More specifically: given a pair of large primes p and q, a decent computer can, in general, calculate $m = pq$ quite easily, even if p and q have hundreds of digits. But given only the product m of two such prime numbers, it's generally *not so easy*, even with *lots* of computing power, to figure out of which two primes m is a product (even with the advance knowledge that m *is*, in fact, a product of *some* pair of primes).

For example, Mathematica 13.3.1.0, running on an M1 iMac, took 0.000012 seconds of CPU time to multiply together the primes

$$p = 28{,}012{,}569{,}795{,}147{,}037{,}305{,}920{,}963{,}277{,}749{,}628{,}914{,}662{,}527{,}590{,}314{,}892{,}381{,}540{,}899{,}557{,}658{,}727{,}561{,}627{,}073{,}596{,}629{,}516{,}007{,}733{,}350{,}970{,}901{,}196{,}381{,}503{,}333{,}712{,}077{,}626{,}705{,}499{,}954{,}515{,}577{,}260{,}792{,}348{,}632{,}533{,}889{,}368{,}689{,}260{,}551$$

and

$$q = 409{,}979{,}012{,}803{,}156{,}684{,}026{,}992{,}824{,}311{,}225{,}162{,}850{,}617{,}662{,}647{,}990{,}082{,}269{,}707{,}895{,}322{,}401{,}233{,}158{,}338{,}554{,}223{,}937{,}364{,}652{,}604{,}454{,}924{,}195{,}546{,}130{,}462{,}715{,}574{,}033{,}228{,}042{,}504{,}577{,}902{,}809{,}413{,}850{,}720{,}086{,}027{,}157{,}221{,}973{,}957{,}611{,}016{,}318{,}502{,}032{,}623{,}823.$$

(Both p and q *are*, in fact, prime.) It's been working on factoring $m = pq$ since approximately 10 AM on Tuesday, November 12, and is not likely to succeed. You'll be notified if it does. (It won't.)

Here is how RSA works.

Part A: Encoding. We start with a message; we'll assume, for the sake of simplicity, that the message consists only of upper-case English letters A, B, . . . , Z. We encode our message as follows.

1. First, we convert the message to a natural number n. To do so, we'll use this "numerization key:"

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

For example, the message "HI" would become the integer $n = 1819$.

Remark: A more complex message might involve digits, lower-case letters, punctuation, spaces, etc. We could numerize those symbols as well; there are plenty of two-digit numbers left to numerize symbols with. But to keep things simple, we'll assume, again, that we're working only with the symbols A through Z.

Also, the numerization code is easily cracked; it should not be considered a fundamental part of the RSA encryption scheme. Rather, it's just a simple way of putting everything into the form of an integer, so that we may perform the "integer arithmetic" to be described below.

2. Next, we raise the natural number n to another natural number k. For example, if $n = 1819$ as above, and we choose $k = 17$, then

$$n^k = 1819^{17} = 26{,}130{,}991{,}223{,}692{,}189{,}568{,}654{,}731{,}688{,}484{,}952{,}572{,}018{,}097{,}043{,}964{,}584{,}557.$$

3. Next, we choose *another* natural number m, and divide m into n^k, yielding a quotient q and a remainder r, where $0 \leq r < m$. That is, we write

$$n^k = m \cdot q + r \qquad (0 \leq r < m). \tag{1}$$

By the division algorithm, the numbers q and r here are uniquely determined.

For example, if n and k are as above and we choose $m = 8927$, then one can compute that

$$\begin{aligned} n^k &= 1819^{17} \\ &= 8927 \cdot 2{,}927{,}186{,}201{,}825{,}046{,}457{,}862{,}745{,}792{,}369{,}771{,}767{,}897{,}176{,}772{,}035{,}911 + 7042, \end{aligned} \tag{2}$$

so our remainder r, in this case, is $r = 7042$.

4. The encoded message, then, *is* the remainder r. So again, in the above example, the encoded version of the original message "HI" (or its "numerized" alias 1819) is 7042.

We used a computer to get the equation (**??**). For smallish numbers, even a pocket calculator will work: see the Exercises at the end of this section.

In real-life implementation of RSA, the numbers n, k, and m will typically be *much* bigger, and therefore the calculations required to find r will be unmanageable on a computer, even a very powerful one, without some added "tricks."

To move towards an understanding of such tricks, note that equation (**??**) above tells us that

$$1819^{17} - 7042 = 8927 \cdot 2{,}927{,}186{,}201{,}825{,}046{,}457{,}862{,}745{,}792{,}369{,}771{,}767{,}897{,}176{,}772{,}035{,}911,$$

which in turn tells us that

$$8927 | (1819^{17} - 7042). \tag{3}$$

More generally, equation (**??**) above tells us that

$$n^k - r = m \cdot q,$$

which in turn tells us that

$$m|(n^k - r).$$

The moral of the story is that we should be studying phenomena of the form $m|(a-b)$. We do so in the next section.

Exercises for Part A. You'll need a calculator for these exercises.

1. (a) Numerize the single-letter message "L," using the numerization key above. Call your numerization n: $n =$ ___22___.

   (b) Compute n^k, with $k = 5$. Just plug n^k into your calculator, and write down the number you get. Answer: $n^k =$ ___5,153,632___.

   (c) Let $m = 577$. Find natural numbers q and r, with $0 \leq r < m$, such that $n^k = m \cdot q + r$. Hint: plug n^k/m into your calculator. Write your answer in decimal form:

   $n^k/m =$ ___8931.771231___.

   Your answer should have some stuff to the left of the decimal, and some stuff to the right: that is, your answer should look like $q.y$, where q and y are natural numbers. Then q *is* your quotient q. To find your remainder r, subtract $m \cdot q$ from n^k.
   Write your answer here:

   $n^k = 577 \cdot$ ___8931___ $+$ ___445___.

2. Repeat problem 1 with the message "A," the exponent $k = 7$, and the divisor $m = 223$:

   $n =$ ___11___; $n^k =$ ___19,487,171___; $n^k/m =$ ___87,386.41704___;
   $n^k = 223 \cdot$ ___87,386___ $+$ ___93___.

3. Repeat problem 1 with the message "ME," the exponent $k = 2$, and the divisor $m = 1137$:

   $n =$ ___2,315___; $n^k =$ ___5,359,225___; $n^k/m =$ ___4,713.478452___;
   $n^k = 1137 \cdot$ ___4,713___ $+$ ___544___.

Part B: Congruences. As noted near the end of Part A, it will be useful to consider how to treat situations where $m|(a-b)$, for integers a, b, m. To this end, we begin with:

Definition 1. Let $a, b, m \in \mathbb{Z}$. We say "a is congruent to b mod m," and write

$$a \equiv b \pmod{m},$$

if $m|(a-b)$.

For example:

$$\begin{aligned}
31 &\equiv 1 \pmod{10} && \text{(since } 31-1 = 10\cdot 3\text{, so } 10|(31-1)\text{);}\\
3^5 &\equiv 3 \pmod{24} && \text{(since } 3^5-5 = 240 = 24\cdot 10\text{, so } 24|(3^5-5)\text{);}\\
132617 &\equiv 617 \pmod{132} && \text{(since } 132617-617 = 132000 = 132\cdot 1{,}000\text{);}\\
-24 &\equiv 48 \pmod{9} && \text{(since } -24-48 = 72 = 9\cdot 10\text{);}\\
k &\equiv 1 \pmod{2} && \text{if } k \text{ is odd, since then } k-1 \text{ is divisible by 2;}\\
1819^{17} &\equiv 7042 \pmod{8927} && \text{(by equation (\textbf{??}) above);}\\
732597^{48} &\equiv 1 \pmod{65} && \text{(we'll see why in Part D below);}
\end{aligned}$$

and so on.

In general, a relation of the form $a \equiv b \pmod{m}$ is called a *congruence*. In such a congruence, we call m the *modulus*. And when manipulating congruences, we say that we are doing *modular arithmetic*.

In the next section, we'll need to do a fair amount of modular arithmetic. The following proposition will allow us to do so.

Proposition 1.

(a) Let $a, b, c, m \in \mathbb{Z}$. Then

$$a \equiv b \pmod{m} \quad \text{and} \quad b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}.$$

(b) Let $a, b, c, d, m \in \mathbb{Z}$. Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then:

(i) $a + c \equiv b + d \pmod{m}$;

(ii) $a - c \equiv b - d \pmod{m}$;

(iii) $ac \equiv bd \pmod{m}$.

Proof.

(a) Let $a, b, c, m \in \mathbb{Z}$, and suppose that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Then by definition of congruence, $m|(a-b)$ and $m|(b-c)$. But then m divides the sum $(a-b)+(b-c)$; that is, $m|(a-c)$. So $a \equiv c \pmod{m}$.

(b) (Part (b)(i) only; for the rest, see the Part B Exercises below.) Assume $a, b, c, d, m \in \mathbb{Z}$, $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$. Then by definition of congruence, $m|(a-b)$ and $m|(c-d)$. So $m|\big((a-b)+(c-d)\big)$ or, rearranging terms, $m|\big((a+c)-(b+d)\big)$. But then, by definition of congruence, $a + c \equiv b + d \pmod{m}$. □

Remark. In this proof, we've used the results Exercise B(i)-3 in S-POP. You may use these results in the Exercises below. You don't need to cite that S-POP Exercise directly, as long as you use it properly.

Example 1. We can compute that $46 \equiv -6 \pmod{13}$ and $63 \equiv -2 \pmod{13}$. By part (b)(i) of the above proposition, we can add these two congruences together to get

$$109 \equiv -8 \pmod{13},$$

which we can check by noting that $109 - (-8) = 117 = 13 \cdot 9$.

Example 2. Suppose we want to compute the remainder of $11^4 \pmod{57}$, by which we mean the remainder of 11^4 after division by 57. We first note that $11^2 = 121$, and we compute easily that $121 = 57 \cdot 2 + 7$, so $11^2 \equiv 7 \pmod{57}$. But by part (iii) of the above proposition, we can multiply this congruence by itself, to get

$$11^2 \cdot 11^2 \equiv 7 \cdot 7 \pmod{57},$$

or

$$11^4 \equiv 49 \pmod{57}.$$

This last identity tells us that $11^4 = 57 \cdot q + 49$ for some integer q. And since $0 \leq 49 < 57$, we see that 49 must be the remainder of $11^4 \pmod{57}$.

This method is, arguably, easier than actually trying to divide 57 into 11^4 directly.

Example 3. What is the remainder of $11^8 \pmod{57}$? Well, by Example 2 directly above, $11^4 \equiv 49 \pmod{57}$, so by the same kind of argument as was used in that example,

$$11^4 \cdot 11^4 \equiv 49 \cdot 49 \pmod{57},$$

meaning

$$11^8 \equiv 2401 \pmod{57}.$$

Now 2401 is larger than 57, so 2401 can't be a remainder after division by 57. But we can easily divide 57 into 2401: we compute that $2401 = 57 \cdot 42 + 7$, so

$$2401 \equiv 7 \pmod{57}.$$

By part (a) of Proposition 1 above, we can string together the above two congruences $11^8 \equiv 2401 \pmod{57}$ and $2401 \equiv 7 \pmod{57}$ to get

$$11^8 \equiv 7 \pmod{57}.$$

Since 7 *is* less than 57, 7 *is* our remainder (mod 57).

Exercises for Part B.

1. Use your answers to the Exercises for Part A, above, to fill in each of the following blanks:

   (a) $22^5 \equiv$ ___445___ (mod 577).

   (b) $11^7 \equiv$ ___93___ (mod 223).

   (c) $2315^2 \equiv$ ___544___ (mod 1137).

2. Use the methods and results of Examples 2 and 3 in Part B above to compute the remainder of $11^{16} \pmod{57}$.

   In Example 3 we computed that $11^8 \equiv 7 \pmod{57}$. But then $11^{16} = \left(11^8\right)^2 \equiv 7^2 = 49 \pmod{57}$.

3. Prove parts (b)(ii,iii) of Proposition 1 above.

   Hint for part (b)(ii): $m|(a-b)$ and $m|(c-d)$, so $m|\big((a-b)-(c-d)\big)$.

   Hint for part (b)(iii): $m|(a-b)$ and $m|(c-d)$, so $m|\big(c(a-b)+b(c-d)\big)$.

Proof of part (b)(ii): Suppose $a,b,c,d \in \mathbb{Z}$, $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$. Then, by definition of "(mod m)," $m|(a-b)$ and $m|(c-d)$. But then m divides the difference of $(a-b)$ and $(c-d)$; that is, $m|\big((a-b)-(c-d)\big)$. Rearranging terms, we see that this is the same as $m|\big((a-c)-(b-d)\big)$. But then, by definition of "(mod m)," we see that $a-c \equiv b-d \pmod{m}$, as required.

Proof of part (b)(iii): Suppose $a,b,c,d \in \mathbb{Z}$, $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$. Then, by definition of "(mod m)," $m|(a-b)$ and $m|(c-d)$. But then m divides $c(a-b)$ and $b(c-d)$, so m divides the sum $c(a-b)+b(c-d)$. Canceling and rearranging terms, we see that this is the same as $m|(ac-bd)$. But then, by definition of "(mod m)," we see that $ac \equiv bd \pmod{m}$, as required. □

Part C: Successive squaring.

In the Exercises for Part A, above, we described a method for obtaining remainders (mod m). This method works fine for numbers n and k that are relatively small. But it fails when these numbers are in, say, the hundreds of digits. This is because, for numbers n and k of such a magnitude, n^k can be astronomical, to the point where even the best of computers can't compute it explicitly. So for such numbers, we need another strategy.

The strategy that we develop here builds on the techniques of Examples 2 and 3 from Part B above. The important idea behind those examples is that of "successive squaring."

Among other things we saw, in those examples, that we could compute $11^8 \pmod{57}$ without ever having to deal with a number as large as 11^8 *explicitly*. We were able to do so by first computing $11^2 \pmod{57}$, then using this information to compute $11^4 \pmod{57}$, and finally using that information, in turn, to compute $11^8 \pmod{57}$. And the largest number we had to encounter explicitly, in these investigations, was 2401, which is much smaller than $11^8 = 214358881$.

A similar, but somewhat expanded, strategy will allow us to compute n^k efficiently, even for numbers n and k in the hundreds of digits. We will illustrate this strategy, below, with substantially smaller numbers n and k, so that we can do most of the computations "by hand" (or at worst with a pocket calculator). But the same ideas apply to much much larger numbers.

Example 1. Compute $13^{27} \pmod{15}$.

Solution. Our method here will comprise three main steps.

Step 1: We compute the "binary expansion" of the exponent 27. That is, we express 27 as a sum of powers of 2. Such an expansion of a natural number k always exists.

To compute the binary expansion of 27, we first ask: what's the largest power of 2 that "goes into" 27, in the sense of being less than 27? In this case, the answer is $16 = 2^4$. Subtract that power of 2 from 27 to get 11, and ask: what's the largest power of 2 that goes into 11? The answer is $8 = 2^3$. Subtract 8 from 11 to get 3, and ask: a what's the largest power of 2 that goes into 3? The answer is $2 = 2^1$. Subtract 2 from 3 to get $1 = 2^0$, and we're done: we've found that

$$27 = 16 + 8 + 2 + 1.$$

To summarize our thought process: we computed that

$$27 = 16 + 11 = 16 + 8 + 3 = 16 + 8 + 2 + 1.$$

We kept "breaking off" powers of 2 until there were none left to break off.

Step 2. Make a list of the base, 13, raised to successive powers of 2 (starting with $2^0 = 1$), (mod 15). Keep going until you've raised the base to the largest power of 2 appearing in Step 1. Each entry in the list is found by squaring, and reducing (mod 15), the previous entry, as follows.

$$\begin{aligned} 13 &\equiv 13 \pmod{15}, \\ 13^2 &\equiv 169 \equiv 15 \cdot 11 + 4 \equiv 4 \pmod{15}, \\ 13^4 &\equiv (13^2)^2 \equiv 4^2 \equiv 16 \equiv 1 \pmod{15}, \\ 13^8 &\equiv (13^4)^2 \equiv 1^2 \equiv 1 \pmod{15}, \\ 13^{16} &\equiv (13^8)^2 \equiv 1^2 \equiv 11 \pmod{15}. \end{aligned}$$

Step 3. Put Steps 1 and 2 together to compute $13^{27} \pmod{15}$, reducing along the way. Like this:

$$\begin{aligned} 13^{27} &\equiv 13^{16+8+2+1} \equiv 13^{16} \cdot 13^8 \cdot 13^2 \cdot 13^1 \\ &\equiv 1 \cdot 1 \cdot 4 \cdot 13 \equiv 52 \equiv 15 \cdot 3 + 7 \equiv 7 \pmod{15}. \end{aligned}$$

To summarize the strategy for finding $n^k \pmod{m}$:

- **Step 1.** Compute the binary expansion of k (write k as a sum of powers of 2, including, if necessary, the power $2^0 = 1$).
- **Step 2**. Make a list of the base n raised to successive powers of 2 (starting with $2^0 = 1$), (mod m). Keep going until you've raised n to the largest power of 2 appearing in Step 1. Each entry in the list is found by squaring, and reducing (mod m), the previous entry.
- **Step 3.** Put Steps 1 and 2 together to compute n^k (mod m), reducing along the way to keep numbers small.

Here's another example.

Example 2. Compute 24^{37} (mod 57).

Solution. Step 1: Compute the "binary expansion" of the exponent 37:

$$37 = 32 + 4 + 1.$$

Step 2. Raise the base 24 to successive powers of 2, (mod 57). Keep going through the largest power of 2 – namely, 32 – appearing in Step 1:

$$\begin{aligned}
24 &\equiv 24 \pmod{57},\\
24^2 &\equiv 576 \equiv 57\cdot 10 + 6 \equiv 6 \pmod{57},\\
24^4 &\equiv (24^2)^2 \equiv 6^2 \equiv 36 \pmod{57},\\
24^8 &\equiv (24^4)^2 \equiv 36^2 \equiv 1296 \equiv 57\cdot 22 + 42 \equiv 42 \pmod{57},\\
24^{16} &\equiv (24^8)^2 \equiv 42^2 \equiv 1764 \equiv 57\cdot 30 + 42 \equiv 54 \pmod{57},\\
24^{32} &\equiv (24^{16})^2 \equiv 54^2 \equiv 2916 \equiv 57\cdot 51 + 9 \equiv 9 \pmod{57}.
\end{aligned}$$

Step 3. Put Steps 1 and 2 together to compute 24^{37} (mod 57), reducing along the way to keep numbers small. Like this:

$$\begin{aligned}
24^{37} &\equiv 24^{32+4+1} \equiv 24^{32}\cdot 24^4 \cdot 24^1\\
&\equiv 9\cdot 36\cdot 24 \equiv 324\cdot 24 \equiv (57\cdot 5 + 39)\cdot 24\\
&\equiv 39\cdot 24 \equiv 936 \equiv 57\cdot 16 + 24 \equiv 24 \pmod{24}.
\end{aligned}$$

Note that, in Steps 2 and 3 of Example 2 directly above, we had to compute some remainders that weren't immediately obvious. For such remainders, one can use the method of the Exercises from Part A above.

For example, we computed in Step 2 above that $2916 \equiv 57\cdot 51 + 9 \equiv 9$ (mod 57). How did we find this? We divided 2916 by 57 on a calculator: we got $2916/57 = 51.15789474$. This tells us that the quotient q is 51: that is, $2916 = 57 \cdot 51 + r$, where r is the desired remainder. To find r, we now just subtract: $r = 2916 - 57 \cdot 51 = 9$. So $2916 = 57 \cdot 51 + 9$, so $2916 \equiv 9 \pmod{57}$.

We also note that, in Steps 2 and 3 of both examples above, we used the symbol "$\equiv$" exclusively, even though we could have used "$=$" in some places. For example, we wrote $24^{37} \equiv 24^{32+4+1}$, even though both sides are, in fact, equal. It's safe to use "$\equiv$" always, when computing an answer (mod m), since if two numbers are equal, they're certainly congruent (mod m), for any $m \in \mathbb{Z}$ (since $a = b \Rightarrow a - b = 0 \Rightarrow m|(a-b) \Rightarrow a \equiv b \pmod{m}$, no matter what m is).

It's not always safe to go the other way though: we can certainly have $a \equiv b \pmod{m}$ without having $a = b$.

Exercises for Part C.

Using the method of successive squaring:

1. Compute $3^{42} \pmod{15}$.

Solution. Step 1: Compute the binary expansion of the exponent 42:

$$42 = 32 + 8 + 2.$$

Step 2. Raise the base 3 to successive powers of 2, (mod 15). Keep going through the largest power of 2 – namely, 32 – appearing in Step 1:

$$\begin{aligned}
3 &\equiv 3 \pmod{15},\\
3^2 &\equiv 9 \pmod{15},\\
3^4 &\equiv (3^2)^2 \equiv 9^2 \equiv 81 \equiv 15 \cdot 5 + 6 \equiv 6 \pmod{15},\\
3^8 &\equiv (3^4)^2 \equiv 6^2 \equiv 36 \equiv 6 \pmod{15},\\
3^{16} &\equiv (3^8)^2 \equiv 6^2 \equiv 36 \equiv 6 \pmod{15},\\
3^{32} &\equiv (3^{16})^2 \equiv 6^2 \equiv 36 \equiv 6 \pmod{15}.
\end{aligned}$$

Step 3. Put Steps 1 and 2 together to compute $3^{42} \pmod{15}$, reducing along the way to keep numbers small. Like this:

$$\begin{aligned}
3^{42} &\equiv 3^{32+8+2} \equiv 3^{32} \cdot 3^8 \cdot 3^2\\
&\equiv 6 \cdot 6 \cdot 9 \equiv 6 \cdot 54 \equiv 6 \cdot (15 \cdot 3 + 9) \equiv 6 \cdot 9 \equiv 54 \equiv 15 \cdot 3 + 9 \equiv 9 \pmod{15}.
\end{aligned}$$

2. Compute $27^{84} \pmod{38}$.

Solution. Step 1: Compute the binary expansion of the exponent 84:

$$84 = 64 + 16 + 4.$$

Step 2. Raise the base 27 to successive powers of 2, (mod 38). Keep going through the largest power of 2 – namely, 64 – appearing in Step 1:

$$\begin{aligned}
27 &\equiv 27 \pmod{15},\\
27^2 &\equiv 729 \equiv 38 \cdot 19 + 7 \equiv 7 \pmod{38},\\
27^4 &\equiv (27^2)^2 \equiv 7^2 \equiv 49 \equiv 11 \pmod{38},\\
27^8 &\equiv (27^4)^2 \equiv 11^2 \equiv 121 \equiv 38 \cdot 3 + 7 \equiv 7 \pmod{38},\\
27^{16} &\equiv (27^8)^2 \equiv 7^2 \equiv 49 \equiv 11 \pmod{38},\\
27^{32} &\equiv (27^{16})^2 \equiv 11^2 \equiv 121 \equiv 7 \pmod{38},\\
27^{64} &\equiv (27^{32})^2 \equiv 7^2 \equiv 49 \equiv 11 \pmod{38}.
\end{aligned}$$

Step 3. Put Steps 1 and 2 together to compute $27^{84} \pmod{38}$, reducing along the way to keep numbers small. Like this:

$$\begin{aligned}
27^{84} &\equiv 27^{64+16+4} \equiv 27^{64} \cdot 27^{16} \cdot 27^4\\
&\equiv 11 \cdot 11 \cdot 11 \equiv 121 \cdot 11 \equiv 7 \cdot 11 \equiv 77 \equiv 38 \cdot 2 + 1 \equiv 1 \pmod{38}.
\end{aligned}$$

3. Numerize the message “HI,” using the numerization key on the first page, and encode it using the exponent $k = 17$ and the modulus $m = 8927$. Note: you’ll come up with some relatively large numbers here, which you may want to reduce $\pmod{m}$ in the way described in the Exercises for Part A.

For example, you will have to reduce $1819^2 \pmod{8927}$. Type $1819^2/8927$ into your calculator to get something like $370.646\ldots$. So your quotient is 370. Then enter $1819^2 - 8927 \cdot 370$, to get 5771, so 5771 is your remainder, so $1819^2 \equiv 5771 \pmod{8927}$. And so on.

You might want to check your answer against equation (**??**) on page 2 of these Notes.

Solution. HI→ 1819.

Step 1: Compute the binary expansion of 17:

$$17 = 16 + 1.$$

Step 2. Raise 1819 to successive powers of 2, (mod 8927).

$$\begin{aligned}
1819 &\equiv 1819 \pmod{8927},\\
1819^2 &\equiv 8927 \equiv 38 + 5771 \equiv 5771 \pmod{8927},\\
1819^4 &\equiv (1819^2)^2 \equiv 5771^2 \equiv 8927 \cdot 3730 + 6731 \pmod{8927} \equiv 6731 \pmod{8927},\\
1819^8 &\equiv (1819^4)^2 \equiv 6731^2 \equiv 8927 \cdot 5075 + 1836 \pmod{8927} \equiv 1836 \pmod{8927},\\
1819^{16} &\equiv (1819^8)^2 \equiv 1836^2 \equiv 8927 \cdot 377 + 5417 \pmod{8927} \equiv 5417 \pmod{8927}.
\end{aligned}$$

Step 3. Put Steps 1 and 2 together to compute $1819^{17} \pmod{8927}$:

$$\begin{aligned} 1819^{17} &\equiv 1819^{16+1} \equiv 1819^{16} \cdot 1819 \\ &\equiv 5417 \cdot 1819 \equiv 8927 \cdot 1103 + 7042 \equiv 7042 \pmod{8927}. \end{aligned}$$