Notes on the RSA Algorithm (a.k.a. "RIZZ")

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): This is very similar to the proof of part (b)(i), given above.

   Hint for part (b)(iii): Write $a - b = m \cdot q$ and $c - d = m \cdot s$ for integers q and s (explain why you can do this). Now note that

   $$ac - bd = c(a - b) + b(c - d).$$

   Given this, write $ac - bd$ as a multiple of m.

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 $m|(c - d)$. So $a - b = m \cdot q$ and $c - d = m \cdot s$ for some q,$s \in \mathbb{Z}$. But then

$$(a - c) - (b - d) = a - c - b + d = (a - b) - (c - d) = m \cdot q - m \cdot s = m(q - s),$$

and since $q - s$ is an integer, we see that $m|\big((a-c)-(b-d)\big)$. 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 $m|(c - d)$. So $a - b = m \cdot q$ and $c - d = m \cdot s$ for some q,$s \in \mathbb{Z}$. But then

$$ac - bd = c(a - b) + b(c - d) = c(m \cdot q) + b(m \cdot s) = m(cq + bs),$$

and since $cq + bs$ is an integer, we see that $m|\big(ac - bd\big)$. But then, by definition of "(mod m)," we see that $ac \equiv bd \pmod{m}$, as required. $\square$

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} (mod 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 (mod m) in the way described in the Exercises for Part A.

For example, you will have to reduce 1819^2 (mod 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 $1819^2 \equiv 5771$ (mod 8927). And so on.

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

Solution. HI$\to$ 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} (mod 8927):

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