

Here are some solutions to homework problems:

**RSA 1.**

1. Working mod 10:  $15^{21} \equiv 5^{21}$ ;  $5^{21} \equiv (5^{10})^2 \cdot 5$ ;  $5^{10} \equiv (5^5)^2$ ;  $5^5 \equiv (5^2)^2 \cdot 5$ ;  
 $5^2 \equiv 25 \equiv 5$ ;  $5^5 \equiv (5^2)^2 \cdot 5 \equiv 5 \cdot 5 \equiv 5$ ;  $5^{10} \equiv (5^5)^2 \equiv 5^2 \equiv 5$ ;  $5^{21} \equiv (5^{10})^2 \cdot 5 \equiv 5$ .
2. Working mod 100:  $15^{21} \equiv (15^{10})^2 \cdot 15$ ;  $15^{10} \equiv (15^5)^2$ ;  $15^5 \equiv (15^2)^2 \cdot 15$ ;  
 $15^2 \equiv 15 \cdot 15 \equiv 25$ ;  $15^5 \equiv 25 \cdot 25 \cdot 15 \equiv 75$ ;  $15^{10} \equiv 75^2 \equiv 25$ ;  $15^{21} \equiv 25^2 \cdot 15 \equiv 75$ .

Here is a slightly different variation on the repeated squaring method:

3. Working mod 52:  $20^2 \equiv 400 \equiv 36$ ;  $20^4 \equiv 36^2 \equiv 1296 \equiv 48$ ;  $20^8 \equiv 48^2 \equiv 2304 \equiv 16$ ;  $20^{16} \equiv 16^2 \equiv 256 \equiv 48$ ;  $20^{32} \equiv 48^2 \equiv 2304 \equiv 16$ ; So  
 $20^{36} \equiv 20^{32} \cdot 20^4 \equiv 16 \cdot 48 \equiv 768 \equiv 40$ .
4. Working mod 52: Using the either of the methods above, we find that  
 $2^{35} \equiv 20$ .
5. Again, working mod 52: Since  $50 \equiv -2$ ,  $50^{36} \equiv (-2)^{36} \equiv -(2)^{36} \equiv -20 \equiv 32$ .

**RSA 2.** A key (private or public) in an RSA system must have an inverse mod  $(p-1)(q-1)$ .  $d$  has an inverses mod  $(p-1)(q-1)$  if and only if  $\gcd(e, (p-1)(q-1)) = 1$ . So the only one possible in our list is 25 since  $(p-1)(q-1) = 12 \cdot 16 = 192$ .

The information to publish is  $pq$ , which is 221, and the encoding key, which is the inverse of 25 mod 192. The inverse of 25 mod 192 is 169.

20 gets coded as  $20^{169} \bmod 221$ , which is 150. 20 gets decoded as  $30^{25} \bmod 221$ , which is 30. (Note: this is not a good thing! Why not?)

I appologize for the large size of 169, but here are some ways to compute  $20^{169}$  by hand (with the aid of a calculator):

- First notice that  $169 = 1 + 168 = 1 + (4)(6)(7)$ . So working mod 221:

$$\begin{aligned} 20^{169} &\equiv (((20^7)^6)^4) \cdot 20 \\ 20^7 &\equiv 1280000000 \equiv 45 \\ 45^6 &\equiv 8303765625 \equiv 25 \\ 25^4 &\equiv 390625 \equiv 118 \\ \text{so } 20^{169} &\equiv 118 \cdot 20 \equiv 2360 \equiv 150 \end{aligned}$$

If some of these numbers are too big for your calculator, you can use  $169 = 1 + 7(3)(2)(4)$  and start by using  $20^7 = 20^4 \cdot 20^3$ . If you can handle somewhat larger numbers, using  $169 = (13)(13)$  is even better. Notice that this uses the same basic ideas as repeated squaring.

- Use Fermat's little Theorem: First determine  $20^{169} \pmod{13}$  and  $\pmod{17}$  separately, then combine.

$$\text{Mod } 13: 20^{169} \equiv 7^{12(14)+1} \equiv 1^{14} \cdot 7 \equiv 7.$$

$$\text{Mod } 17: 3^{169} \equiv 3^{16(10)+9} \equiv 1^0 \cdot 3^9 \equiv 3^9 \equiv 14.$$

By the Chinese Remainder Theorem, we can figure out that  $20^{169} \pmod{221} = 150$ .

**RSA 3.** This is a Chinese Remainder Theorem Problem. Set things up by writing

$$x = 42B_1 + 35B_2 + 30B_3$$

Reading this equation mod 5,6, and 7 gives:

$$x \equiv 42B_1 \equiv 2 \pmod{5}$$

$$x \equiv 35B_2 \equiv 3 \pmod{6}$$

$$x \equiv 30B_3 \equiv 4 \pmod{7}$$

So we solve these three equations using the inverses listed to the right:

$$\begin{array}{ll} 2B_1 \equiv 2 \pmod{5} & [2 \cdot 3 \equiv 1 \pmod{5}] \\ (-1)B_2 \equiv 3 \pmod{6} & [-1 \cdot (-1) \equiv 1 \pmod{6}] \\ 2B_3 \equiv 4 \pmod{7} & [2 \cdot 4 \equiv 1 \pmod{7}] \end{array}$$

The result is

$$\begin{array}{ll} 3 \cdot 2 \cdot B_1 \equiv 3 \cdot 2 \pmod{5} \\ (-1)(-1)B_2 \equiv (-1)3 \pmod{6} \\ (4)2B_3 \equiv (4)4 \pmod{7} \end{array}$$

So  $B_1 = 1$ ,  $B_2 = -3$  and  $B_3 = 2$  will produce  $x = 42 - 3(35) + 2(30) = -3$ . [Now we see that we could have noticed this from the very start, why?] Of course,  $-3$  is not positive. To other values that work, we may add any multiple of  $5 \cdot 6 \cdot 7 = 210$ . So the smallest positive number is 207.

**RSA 4.** Here is output from the Euclid's Algorithm webpage:

$$\begin{array}{ll} +290 = 2 * +143 + +4 & +4 = +1 * +290 + -2 * +143 \\ +143 = 35 * +4 + +3 & +3 = -35 * +290 + +71 * +143 \\ +4 = 1 * +3 + +1 & +1 = +36 * +290 + -73 * +143 \\ +3 = 3 * +1 + +0 & +0 = -143 * +290 + +290 * +143 \end{array}$$

It is a little hard to read, but the point is that by backsubstituting in Euclid's Algorithm, we find that

$$1 = (36)290 + (-73)143$$

Considering this equation mod 290, we see that  $1 \equiv (-73)(143)$ , so  $-73$  and  $143$  are inverses. Of course,  $-73 \equiv 290 - 73 \equiv 217$ .