SOLUTIONS
Math 345
Homework 9
11/8/2017

Exercise 32. Find one solution to the following congruences. Make a careful and detailed list of each of your steps. You may use a computer to do any of the intermediate computations.

(a) $x^{329} \equiv 452 \pmod{1147}$

Answer. **Compute $\phi(n)$:** We have $1147 = 31 * 37$, so that $\phi(1147) = 30 * 36 = 1080$. **Compute $k^{-1} \pmod{\phi(n)}$:** Using the Euclidean algorithm, we can compute $1080 * 46 + 329 * (-151) = 1$. So

$$329 * (-151) \equiv_{1080} 1, \quad \text{i.e. } 329^{-1} \equiv_{1080} -151 \equiv_{1080} 929 = u.$$

Compute $b^u \pmod{n}$: Using the method of successive squaring, we have

$$929 = 2^9 + 2^8 + 2^7 + 2^5 + 2^0,$$

and

a	0	1	2	3	4	5	6	7	8	9
$\overline{452^{2^{a-1}}}^2$	452	204304	19044	478864	319225	128881	173889	478864	319225	128881
$\overline{452^{2^a}}$	452	138	692	565	359	417	692	565	359	417

So

$$\begin{aligned} x &\equiv_{1147} 452^{929} \\ &\equiv_{1147} 452^{2^9} 452^{2^8} 452^{2^7} 452^{2^5} 452^{2^0} \\ &\equiv_{1147} 417 * 359 * 565 * 417 * 452 \\ &\equiv_{1147} 121 * 376 \equiv_{1147} \boxed{763}. \end{aligned}$$

□

(b) $x^{275} \equiv 139 \pmod{588}$

Answer. **Compute $\phi(n)$:** We have $588 = 2^2 * 3 * 7^2$, so that $\phi(588) = 2 * 2 * 42 = 168$. **Reduce exponent:** Since $275 \equiv_{168} 107$, we have $x^{275} \equiv_{588} x^{107}$. **Compute $k^{-1} \pmod{\phi(n)}$:** Using the Euclidean algorithm, we can compute $107 * 11 + 168 * (-7) = 1$. So

$$107 * 11 \equiv_{168} 1, \quad \text{i.e. } 107^{-1} \equiv_{168} 11 = u.$$

Compute $b^u \pmod{n}$: Using the method of successive squaring, we have

$$11 = 2^3 + 2^1 + 2^0,$$

and

a	0	1	2	3
$\overline{139^{2^{a-1}}}^2$	139	19321	255025	177241
$\overline{139^{2^a}}$	139	505	421	253

So

$$\begin{aligned} x &\equiv_{588} 139^{11} \\ &\equiv_{588} 139^{2^3} 139^{2^1} 139^{2^0} \\ &\equiv_{588} 253 * 505 * 139 \equiv_{588} \boxed{559}. \end{aligned}$$

□

Exercise 33. In Chapter 17, we described how to compute one kth root of b modulo n, but there may be other solutions. For example, if $a^2 \equiv_n b$, then we also have $(-a)^2 \equiv_n b$.

(a) Let b, k, and n be integers that satisfy

$$\gcd(b, n) = 1 \qquad \text{and} \qquad \gcd(k, \phi(n)) = 1.$$

Show that b has exactly one kth root modulo n.
[Hint: You know there's *at least* one, so you just have to show there isn't *more than* one. So start by supposing a and a' are both kth roots of b modulo n, i.e. $a^k \equiv_n b$ and $(a')^k \equiv_n b$. Now use the tools for finding solutions from class to show that $a \equiv_n a'$.]

Proof. We already saw that under these assumption, b has at least one kth root mod n. Now suppose that a and a' are both kth roots of b modulo n. Since $\gcd(k, \phi(n)) = 1$, we can find u and v such that $ku + \phi(n)v = 1$. Eulers theorem tells us that $a^{\phi(n)} \equiv_n 1 \equiv_n (a')^{\phi(n)}$, so we have

$$a = a^{ku+\phi(n)v} = (a^k)^u (a^{\phi(n)})v \equiv b^u * 1^v \equiv b^u \pmod{n}.$$

Similarly, $a' \equiv b^u \pmod{n}$. So $a \equiv a' \pmod{n}$. □

(b) Why doesn't part (a) contradict our example above? Namely why doesn't the fact that there is more than one solution to $a^2 \equiv_n b$ for most n and b provide a counterexample to part (a)?
Answer. For most values of n, we have $2|\phi(n)$, so $\gcd(2, \phi(n)) \neq 1$. □

(c) Look at some examples were n is prime and try to find a formula for the number of kth roots of b modulo n (assuming that it has at least one). (Don't try to prove your formula.)
[Try setting $n = 3, 5$, and 7 and use a computer to compute $a^k \pmod{n}$ for $a = 2, 3, \ldots, n-1$ and $k = 1, 2, \ldots, n-1$. If you need more data, do more prime n's.]
Answer. We will see that b has $\gcd(k, p-1)$ kth roots modulo p. □

Exercise 34. Our method for solving $x^k \equiv_n b$ is first to find positive integers u and v satisfying $ku - \phi(n)v = 1$, and then the solution is $x \equiv_n b^u$. However, we only showed that this works provided that $\gcd(b, m) = 1$, since we used Eulers formula $b^{\phi(n)} \equiv_n 1$.

(a) If n is a product of distinct primes, show that $x \equiv_n b^u$ (with u as above) is always a solution $x \equiv_n b^u$, even if $\gcd(b, n) > 1$.

[Hint: Check that n divides $(b^u)^k - b$ by checking that each prime divisor of n divides $(b^u)^k - b$. To do that, if $p|n$, then break into cases where $p|b$ or $p \nmid b$. If $p|b$, what can you conclude? If $p \nmid b$, check that $p-1|\phi(n)$, and then plug that information into "$ku = \phi(n)v+1$", and compute $(b^u)^k \pmod{p}$ using Fermat.]

Proof. We want to show that $(b^u)^k \equiv b \pmod{n}$, which means we want to check that n divides $(b^u)^k - b$.

First factor n as $n = p_1 p_2 \cdots p_r$, for primes $p_1 < \cdots < p_r$. So we really only need to check that each p_i divides $(b^u)^k - b$. There are two possibilities.

Case 1: p_i divides b. Then p_i divides $(b^u)^k - b$.
Case 2: Second, p_i doesn't divide b. In this case, note

$$\phi(n) = (p_1 - 1)(p_2 - 2) \cdots (p_r - 1),$$

so that $p_i - 1$ divides $\phi(n)$. This means that

$$uk = 1 + \phi(n)v = 1 + (pi - 1)w \quad \text{for some } w.$$

So

$$(b^u)^k = b^{uk} = b \cdot (b^{p_i - 1})w \equiv b \cdot 1^w \equiv b \pmod{p_i}.$$

□

(b) Show that our method does not work for the congruence $x^5 \equiv 6 \pmod 9$ (by finding u and plugging in).

Proof. First, we solve $ku - \phi(n)v = 1$. In our case, $k = 5$, $n = 9$, and $\phi(n) = 6$, so we get $u = 5$ and $v = 4$. Then $b^u = 6^5 \equiv 0 \pmod 9$. But $x = 0$ is not a solution of the congruence $x^5 \equiv 6$ mod 9. (In fact, this congruence doesnt have any solutions.) □

Exercise 35. Decode the following message, which was sent using the modulus $n = 7081$ and the exponent $k = 1789$. (Note that you will first need to factor n.)

5192, 2604, 4222

Answer. We have $7081 = 73 \cdot 97$, so $\phi(7081) = 72 \cdot 96 = 6912$. The least positive value of u which solves $uk + v\phi(n) = 1$ is $u = 85$. Using this, we compute

$$5192u \equiv 1615 \pmod{7081},$$

$$2604u \equiv 2823 \pmod{n},$$

and

$$4222u \equiv 1130 \pmod{n}.$$

So the message is 161528231130, which translates to "Fermat."

□

Exercise 36. It may appear that RSA decryption does not work if you are unlucky enough to choose a message a that is not relatively prime to n. Of course, if $n = pq$ and p and q are large, this is very unlikely to occur. [See Exercise 34.]

(a) Show that in fact RSA decryption does work for all messages a, regardless of whether or not they have a factor in common with n. In other words, show that RSA decryption works for all messages a as long as n is a product of distinct primes.

Answer. This is essentially exercise 34. □

(b) Give an example with $n = 18$ and $a = 3$ where RSA decryption does not work. [Remember, k must be chosen relatively prime to $\phi(n) = 6$.]

Answer. Take $k = 5$.Then $a^k = 35 \equiv 9 \pmod{18}$, so $b = 9$. Next $5k - 4\phi(n) = 1$, so we compute $b^5 = 9^5 \equiv 9 \pmod{18}$. Thus we do not recover the original message $a = 3$. □