Homework 5, MORALLY AND REALLY Due Mar 3

1. (0 points but you have to answer) What is your name? Write it clearly. Staple your HW.

2. (25 points) Martians have a 15 letter alphabet.

   (a) How many shift ciphers can they have?

   (b) How many affine ciphers can they have?

   SOLUTION to 2a: There are 15 shift ciphers, you can shift by 0,1,. . . , 14. Shifting by 0 DOES count.

   SOLUTION to 2b: Affine ciphers are x goes to $ax + b \pmod{15}$. To make this cipher invertible need a rel prime to 15. The following are rel prime to 15: $\{1, 2, 4, 7, 8, 11, 13, 14\}$. There are 8 of those. The b can be anything in $\{0, 1, \ldots, 14\}$. Hence the number of affine ciphers is $8 \times 15 = 120$.

3. (25 points)

   (a) Use the Euclidean algorithm to find the inverse of 81 mod 100. Show all work.

   (b) As you know, there is NO inverse of 45 mod 100. Even so, use the Euclidean algorithm on this problem and show all work. What can you conclude from what you get?

   SOLUTION to 3a

   $100 = 1 \times 81 + 19$

   $81 = 4 \times 19 + 5$

   $19 = 3 \times 5 + 4$

   $5 = 1 \times 4 + 1$.

   We want to express 1 in terms of 100's and 81's. We do this TWO ways.

   METHOD ONE (This is what you learned in class). We work from the bottom up: first expressing 1 in terms of 5 and 4, then express 5 and 4, etc.

   $1 = 5 - 4$. USE $4 = 19 - 3 \times 5$ to obtain

$1 = 5 - 19 + 3 \times 5 = 4 \times 5 - 19$. USE $5 = 81 - 4 \times 19$ to obtain

$1 = 4 \times 5 - 19 = 4 \times (81 - 4 \times 19) - 19 = 4 \times 81 - 17 \times 19$. USE $19 = 100 - 81$ to obtain

$1 = 4 \times 81 - 17 \times 19 = 4 \times 81 - 17 \times (100 - 81) = 21 \times 81 - 17 \times 100$

Now take this equation mod 100 to obtain

$1 \equiv 21 \times 81 \pmod{100}$.

So the inverse of 81 is 21.

METHOD TWO: Work Top Down. Write 19,5,4 in terms of 100's and 81's.

$19 = 100 - 81$.

$5 = 81 - 4 \times 19 = 81 - 4 \times (100 - 81) = 5 \times 81 - 4 \times 100$.

$4 = 19 - 3 \times 5 = (100 - 81) - 3 \times (5 \times 81 - 4 \times 100) = 13 \times 100 - 16 \times 81)$

$1 = 5 - 4 = (5 \times 81 - 4 \times 100) - (13 \times 100 - 16 \times 81) = 21 \times 81 - 17 \times 100$.

SO take the equation $1 = 21 \times 81 - 17 \times 100$ and mod it by 100 to get

$1 \equiv 21 \times 81 \pmod{100}$.

So the inverse of 81 is 21.

VERIFY: $81 \times 21 = (80 + 1)(20 + 1) \equiv 0 + 80 + 20 + 1 \equiv 1$.

SOLUTION TO 3b. Lets TRY to find he inverse of 45 mod 100.

$100 = 2 \times 45 + 10$

$45 = 4 \times 10 + 5$

$10 = 2 \times 5 + 0$.

The last nonzero remainder is 5. So lets try to get 5 as a linear combination of 100's and 45's.

$10 = 100 - 2 \times 45$

$5 = 45 - 4 \times 10 = 45 - 4 \times (100 - 2 \times 45) = 7 \times 45 - 4 \times 100$

Take this last equation mod 100 to get

$5 \equiv 7 \times 45 \pmod{100}$.

Also 5 is the GCD of 45 and 100. This is not a conincidence! We have seen in class that if a and b are nonzero integers with $d = gcd(a, b)$ then

there always exists integers x, y such that $ax + by = d$ (this is known as Bezout's Lemma). The extended Euclidean Algorithm is used to find exactly the value of x and y, regardless of the specific value of d. (We have been using this in the case where $d = 1$ to get inverses.)

4. (25 points)

   (a) Compute $3^{81} \pmod{101}$.

   (b) Compute $7^{1000000000000000} \pmod{101}$.

   SOLUTION TO PROBLEM 4a.

   Note taht since $81 \leq 100$ Fermat's Little Theorem would not help us since it would amountto $3^{81} \equiv 3^{81 \pmod{100}}$ which does not give us a smaller exponent.

   Repeated squaring. First write 81 in base 2. I'll do this slowly:

   The largest power of 2 that is ≤ 81 is 64. Hence

   $81 = 64 + 17$

   The largest powe of 2 that is ≤ 17 is 16. Hence

   $81 = 64 + 16 + 1$.

   So we need 3^1, 3^{16} and 3^{64}. We get these by repeated squaring. All $\equiv$ are mod 101.

   $3^0 \equiv 1$

   $3^1 \equiv 3$

   $3^2 \equiv 9$

   $3^4 \equiv (3^2)^2 \equiv 9^2 \equiv 81$

   $3^8 \equiv (3^4)^2 \equiv 81^2 \equiv (-20)^2 \equiv 400 \equiv 400 - 4(100+1) \equiv 400 - 400 - 4 \equiv -4 \equiv 97$.

   (NOTE: I used that $81 = 101 - 20$ so $81 \equiv -20$ which made me avoid having to do $81 * 81$. I then used

   $$0 \equiv 101 \equiv 4 \times 101 \equiv 4(100 + 1)$$

   to again avoid some calculations.

   $3^{16} \equiv 97^2 \equiv (-4)^2 \equiv 16$

$3^{32} \equiv 16^2 \equiv 256 \equiv 256 - 2(100 + 1) \equiv 56 - 2 \equiv 54$

$3^{64} \equiv 54^2 \equiv 2916 \equiv 88.$

So the answer is 88.

SOLUTION TO 4b

$7^{1000000000000000} \pmod{101}$.

We first mod down the exponent mod 100 using $a^n \equiv a^{n \pmod{p-1}} \pmod{p}$.

So what is $1000000000000000 \equiv 0 \pmod{100}$.

So this is just $7^0 \equiv 1$.