SOLUTIONS
Math 345
Homework 6
10/11/2017

Exercise 23.

(a) Solve the following congruences:

(i) $x^{101} \equiv 7 \pmod{12}$

Answer. We have
$$\phi(12) = \#\{1, 5, 7, 11\}.$$
Since $\gcd(7, 12) = 1$, we must have $\gcd(x, 12) = 1$. So
$$1 \equiv_{12} x^{\phi(12)} = x^4.$$
Therefore
$$7 \equiv_{12} x^{101} = (x^4)^{25}x \equiv_{12} 1 * x = x.$$
So $x = 7$ is a solution.

□

(ii) $10^x \equiv 1 \pmod{27}$

Answer. Since $\gcd(10, 27) = 1$, this has a solution of $x = \phi(27) = \phi(3^3) = 3^2(3-1) = 18$. (There are other solutions as well: e.g. $10^3 = 27 * 37 + 1$.) □

(b) The number 3750 satisfies $\phi(3750) = 1000$. Find an integer $1 \leq a \leq 5000$ that is not a multiple of 7, that satisfies $a \equiv 7^{3003} \pmod{3750}$ [This integer need not be reduced modulo 3750].

Answer. We have
$$a \equiv 7^{3003} \pmod{3750} = (7^{1000})^3)7^3 \equiv 1 * 7^3 \pmod{3750} = 343.$$
This is a multiple of 7, but adding 3750 (which is not a multiple of 7) preserves its residue. So $7^3 + 3750 = 4093$ is one such answer.

□

(c) Show that if $m = 561 = 3 \cdot 11 \cdot 17$, then $a^{m-1} \equiv 1 \pmod{m}$ for all a relatively prime to m. [Hint: There may be 320 values of a between 1 and m that are relatively prime to m, but it is not necessary (nor called for) to actually compute $a^{m-1} \equiv 1 \pmod{m}$ for all those values. Instead, use Fermats Little Theorem to check that $a^{m-1} \equiv 1 \pmod{p}$ for each prime p dividing m, and then explain why this implies that $a^{m-1} \equiv 1 \pmod{m}$.]

Answer. If a is relatively prime to $3 \cdot 11 \cdot 17$, then it is also relatively prime to 3, 11, and 17. So Fermat's little theorem tells us
$$a^2 \equiv 1 \pmod{3}, \qquad a^{10} \equiv 1 \pmod{11}, \qquad \text{and} \qquad a^{16} \equiv 1 \pmod{17}.$$
But 560 is a multiple of all 2, 10, and 16:
$$560 = 2 * 280 = 10 * 56 = 16 * 35.$$
So
$$a^{560} \equiv 1 \pmod{3}, \qquad a^{560} \equiv 1 \pmod{11}, \qquad \text{and} \qquad a^{560} \equiv 1 \pmod{17}.$$
But this means $a^{560} - 1$ is a multiple of 3, 11, and 17. So $a^{560} - 1$ is a multiple of $\mathrm{lcm}(3, 11, 17) = 3 \cdot 11 \cdot 17 = 561$. Therefore $a^{560} \equiv 1 \pmod{561}$, as desired.

See exercise 10.3 in the book. □

Exercise 24. Let $b_1 < b_2 < \cdots < b_{\phi(n)}$ be the integers $1 \leq b_i < n$ that are relatively prime to n, and let $B = b_1 b_2 b_3 \cdots b_{\phi(n)}$ be their product. [This number came up during the proof of Euler's formula.]

(a) Compute B for $n = 4, 5, 6,$ and 8, modulo n. Note that in each case, $B \equiv 1 \pmod{n}$ or $B \equiv n-1 \pmod{n}$, which, together, is the same as $B \equiv \pm 1 \pmod{n}$.

Answer. As in class, let
$$\Phi(n) = \{b_1, b_2, \cdots, b_{\phi(n)}\}.$$

<u>$n = 4$</u>:
Here, $\Phi(4) = \{1, 3\}$. But $3 \equiv -1 \pmod{4}$, so $1 * 3 \equiv_4 1(-1) = -1$.

<u>$n = 5$</u>:
Here, $\Phi(5) = \{1, 2, 3, 4\}$. But $4 \equiv -1 \pmod{5}$ and $2 * 3 \equiv 1 \pmod{5}$, so
$$1 * 2 * 3 * 4 \equiv_5 1 * 1 * (-1) = -1.$$

<u>$n = 6$</u>:
Here, $\Phi(5) = \{1, 5\}$. But $5 \equiv -1 \pmod{6}$, so $1 * 5 \equiv_6 1(-1) = -1$.

<u>$n = 8$</u>:
Here, $\Phi(5) = \{1, 3, 5, 7\}$. But $7 \equiv -1 \pmod{8}$ and $3 * 5 \equiv -1 \pmod{8}$, so
$$1 * 3 * 5 * 7 \equiv_5 1 * (-1) * (-1) = 1.$$

□

(b) Prove that $B \equiv \pm 1 \pmod{n}$ in general. [Hint: Think about multiplicative inverses – when does an integer a have an inverse? How many are there modulo n?]

Proof. = Since a number $1 \leq b < n$ has an inverse modulo n if and only if $\gcd(b, n) = 1$, we have
$$\Phi = \{b_1, b_2, \cdots, b_{\phi(n)}\} = \{1 \leq b < n \mid \ b \text{ has an inverse mod } n\ \}.$$
Now, break Φ into two parts, based on the numbers that are their own inverses and those that are not:
$$\Phi_1 = \{b \in \Phi \mid b^2 \equiv_n 1\} \qquad \Phi_2 = \{b \in \Phi \mid b^2 \neq 1\}$$
(since b is its own inverse if and only if $1 \equiv_n b \cdot b = b^2$). Thus
$$B = \prod_{b \in \Phi} b = \underbrace{\left(\prod_{b \in \Phi_1} b\right)}_{B_1} \underbrace{\left(\prod_{b \in \Phi_2} b\right)}_{B_2}.$$

Of course, if $b \in \Phi_2$, then its unique inverse is in Φ_2 as well:
$$bb' \equiv_n 1 \quad \text{ if and only if } \quad b'b \equiv_n 1.$$
So $B_2 = \prod_{b \in \Phi_2} b = 1$ (each element of Φ_2 has a unique counterpart that it cancels with).

Now what about Φ_1? Well, it turns out that the elements of Φ_1 pair up nicely as well: If $b \in \Phi_1$, then $b^1 = 1$, then

(i) $n - b \in \Phi_1$:
This follows since
$$(n-b)^2 = n^2 - 2bn + b^2 \equiv_n 0 - 0 + 1 = 1.$$

(ii) $b \neq n - b$:
If $b = n - b$, then $2b = n$, so that $b | n$, which contradicts $\gcd(b, n) = 1$.

(iii) $b(n-b) \equiv_n -1$: This follows since

$$b(n-b) = bn - b^2 \equiv_n 0 - 1 = -1.$$

So the elements of Φ_1 break into

$$\Phi_1^{(1)} = \{b \in \Phi \mid b < n/2\} \quad \text{and} \quad \Phi_1^{(2)} = \{b \in \Phi \mid b > n/2\} = \{n - b \mid b \in \Phi_1^{(1)}\}.$$

Thus

$$B_1 = \prod_{b \in \Phi_1} b = \prod_{\substack{b \in \Phi_1 \\ b < n/2}} b(n-b) \equiv (-1)^{|\Phi_1|/2} \pmod{n}.$$

So, finally,

$$B = B_1 B_2 \equiv (-1)^{|\Phi_1|/2} \cdot 1 \pmod{n} = \pm 1.$$

□

(c) Try to find a pattern for when B is equivalent to $+1 \pmod{n}$ and when it is equivalent to $-1 \pmod{n}$. Can you prove your conjecture?

Answer. If $n = 2$, then $B = 1 \equiv_2 -1$. Otherwise, for $n > 2$, it turns out that $B \equiv_n -1$ if and only if there exists a *primitive root* modulo n, which is a number a such that every $b \in \Phi(n)$ can be written as a^k for some k (in group theory, this is what it means for $(\mathbb{Z}/n\mathbb{Z})^\times$ to be cyclic). Note that happens exactly when

$$\{a, a^2, \ldots, a^{\phi(n)}\} \equiv_n \Phi(n) \qquad \text{for some } a \in \Phi(n).$$

In particularly, since $a^{\phi(n)} \equiv_n 1$, and all of the other powers must be distinct, we know

(a) $a^k \equiv_n 1$ if and only if $\phi(n)|k$;

(b) for $1 \leq \ell \leq \phi(n)$, if $a^\ell \not\equiv_n 1$ but $a^{2\ell} \equiv_n 1$, then $a^\ell \not\equiv_n -1$:
We have $\phi(n)|2\ell$. But since $1 \leq \ell \leq \phi(n)$, this means that we must have $\ell = \phi(n)/2$; namely there are only two k for which a^k is it's own inverse. Since 1 and $n-1$ are both in $\Phi(n)$ and are their own inverses, a^ℓ must be the one that's not 1, namely $n-1$, i.e. $-1 \pmod{n}$.

For example, when $n = 5$, take $a = 2$:

$$a^1 = 2, \quad a^2 = 4, \quad a^3 = 8 \equiv_5 3, \quad a^4 = 16 \equiv_5 1;$$

and since $a^{2*2} \equiv_5 1$, we have $a^2 \equiv_5 -1$.

Now, if we're in this case, then

$$B \equiv_n a \cdot a^2 \cdots a^\phi(n) = a^{1+2+\cdots+\phi(n)}.$$

But we showed that

$$1 + 2 + \cdots + \phi(n) = \phi(n)(\phi(n)+1)/2.$$

So $B^2 = a^{\phi(n)+1(\phi(n)+1)} = (a^{\phi(n)})^{\phi(n)+1} \equiv 1^{\phi(n)+1} = 1$. Further, since $\phi(n)$ is even (so that $\phi(n)(\phi(n)+1)/2$ factors into integers as $\phi(n)/2$ and $\phi(n)+1$—see problem 25(b) below) and $\gcd(\phi(n), \phi(n)+1) = 1$, we have $\phi(n) \nmid \phi(n)(\phi(n)+1)/2$. So $B \not\equiv_n 1$. Therefore $B \equiv_n -1$.

Otherwise, one can show that $B \equiv_n 1$ (I'll spare you the proof).

So when is there a primitive root modulo n? We prove in modern algebra that this happens exactly when

$$n = 2, \quad 4, \quad p^k, \quad \text{or} \quad 2p^k$$

for any odd prime p. □

Exercise 25.

(a) Compute $\phi(97)$ and $\phi(8800)$.

Answer. Since 97 is prime and $8800 = 2^5 \cdot 5^2 \cdot 11$, we have

$$\phi(97) = 96 \quad \text{and} \quad \phi(8800) = 2^4(2-1) \cdot 5(5-1) \cdot 10.$$

□

(b) For $n \geq 3$, show $\phi(n)$ is even.

Answer. Factor n into prime powers:

$$n = p_1^{r_1} \cdots p_\ell^{r_\ell}, \quad p_1 < \cdots < p_\ell.$$

If $n = 2^r$ for some $r \geq 2$, then

$$\phi(n) = 2^{r-1}(2-1) = 2^{r-1},$$

which is even since $r - 1 > 0$. Otherwise, p_ℓ is odd, so that $p_\ell - 1$ is even. Thus

$$\phi(n) = \phi(p_1^{r_1}) \cdots \phi(p_\ell)^{r_\ell} = p_1^{r_1-1}(p_1 - 1) \cdots p_\ell^{r_\ell-1}(p_\ell - 1)$$

is even as well. □

(c) Fill in the blank and prove: $\phi(n)$ *is a multiple of 4 if and only if* _______.

Answer. As in the previous part, if n has two odd prime divisors, then $\phi(n)$ will have at least two even factors in $\phi(n) = \phi(p_1^{r_1}) \cdots \phi(p_\ell)^{r_\ell}$, so is a multiple of 4.

Otherwise, $n = 2^r$ or $2^r p^s$ for some odd prime p.

If $n = 2^r$, then $\phi(n) = 2^{r-1}$, which is a multiple of 4 if and only if $r \geq 3$.

If $n = 2^r p^s$ with $r \geq 2$, then $\phi(n) = 2^{r-1}p^{s-1}(p-1)$, which is a multiple of 4 since 2^{r-1} and $p - 1$ are both even.

Finally, if $n = 2p^s$ or p^s, then $\phi(n) = p^{s-1}(p-1)$, which is a multiple of 4 if and only if $p \equiv_4 1$.

In summary, $\phi(n)$ is a multiple of 4 if and only if (1) n has two odd prime divisors, (2) n has a prime divisor $p \equiv_4 1$, or (3) n is a multiple of 4 and has at least one odd prime divisor.

□

(d) Suppose that p_1, p_2, ..., p_r are the distinct primes that divide n (for example, if $n = 7000$, then this list is $2, 5$, and 7). Use what we already know about $\phi(n)$ to prove that

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

Use this formula to double check the value of $\phi(7000)$ (calculated in class), and to compute 1000000. Compare your answer to the other formula for $\phi(n)$.

Answer. We have

$$n = p_1^{k_1} \cdots p_r^{k_r},$$

so

$$\begin{aligned}
n&\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right) \\
&= p_1^{k_1} \cdots p_r^{k_r}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right) \\
&= p_1^{k_1}\left(1 - \frac{1}{p_1}\right) p_2^{k_2}\left(1 - \frac{1}{p_2}\right)\cdots p_r^{k_r}\left(1 - \frac{1}{p_r}\right) \\
&= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})\cdots(p_r^{k_r} - p_r^{k_r-1}) \\
&= \phi(p_1^{k_1} \cdots p_r^{k_r}) = \phi(n),
\end{aligned}$$

as desired. So

$$\phi(7000) = 7000(1 - 1/2)(1 - 1/5)(1 - 1/7) = 7000(1/2)(4/5)(6/7) = 7000(24/70) = 2400.$$

□

(e) Find at least one solution to $x^{8644} = 16 \pmod{2025}$.

Answer. The two prime factors of 2025 are 3 and 5, so

$$\phi(2025) = 2025(2/3)(4/5) = 2025(8/15) = 1080.$$

So since $\gcd(16, 2025) = 1$, we must have $\gcd(x, 2025) = 1$. Therefore, since $8644 \equiv_{1080} 4$, we have

$$16 \equiv_{2025} x^{8644} \equiv_{2025} x^4.$$

One solution to this is $x = 2$.

□

Exercise 26.

(a) Find an x that satisfies both $x \equiv 3 \pmod 7$ and $x \equiv 5 \pmod 9$.

Answer. If $x \equiv 3 \pmod 7$, then $x = 3 + 7y$ for some $y \in \mathbb{Z}$. So

$$5 \equiv_9 x \equiv_9 3 + 7y, \quad \text{i.e.} \quad 7y \equiv_9 2.$$

Since $\gcd(9, 7) = 1$, this has a unique solution. In particular, since

$$4 * 7 = 28 = 3 * 9 + 1 \equiv_9 1,$$

we have

$$y \equiv_9 4 * 7 * y \equiv_9 4 * 2 = 8.$$

So

$$x = 3 + 7 * 8 = \boxed{59}.$$

□

(b) Find an x that satisfies both $x \equiv 3 \pmod{37}$ and $x \equiv 1 \pmod{87}$.

Answer. If $x \equiv 3 \pmod{37}$, then $x = 3 + 37y$ for some $y \in \mathbb{Z}$. So

$$1 \equiv_{87} x \equiv_{87} 3 + 37y, \quad \text{i.e.} \quad 37y \equiv_{87} -2.$$

Since $\gcd(87, 37) = 1$, this has a unique solution. In particular, $y = 7$ is a solution ($7 * 37 = 259 = 3 * 87 - 2$). So

$$x = 3 + 37 * 7 = \boxed{262}.$$

□