SOLUTIONS
Math 345
Homework 5
10/4/2017

Exercise 17. Prove the following.

(a) If $x = x_0$ is a solution to $a + x \equiv b \pmod{n}$, then so is $x = x_0 + kn$ for all $k \in \mathbb{Z}$.

Proof. If $a + x_0 \equiv b \pmod{n}$ and $x = x_0 + kn$, then

$$a + x = a + x_0 + kn \equiv b + 0 \pmod{n} = b.$$

$\square$

(b) If $x = x_0$ is a solution to $ax \equiv b \pmod{n}$, then so is $x = x_0 + kn$ for all $k \in \mathbb{Z}$.

Proof. If $ax_0 \equiv b \pmod{n}$ and $x = x_0 + kn$, then

$$ax = a(x_0 + kn) = ax_0 + akn \equiv b + 0 \pmod{n} = b.$$

$\square$

Exercise 18. For each of the following congruences, decide if there are any solutions. If there are, give a maximal set of distinct (non-congruent) solutions.
[For examples involving numbers larger than 20, use a computer to calculate relevant data to start the problem. For example, in problem (e), you'll use a computer to calculate $\gcd(21, 91)$, as well as one example of $u \in \mathbb{Z}$ such that $21u \equiv \gcd(21, 91) \pmod{91}$. Use functions that allow you to reduce modulo n easily.]

(a) $7x \equiv 3 \pmod{15}$

Answer. Since $\gcd(7, 15) = 1$, there is one answer: since $7 * 13 \equiv_{15} 1$, we have

$$x = 13 \cdot 7x \equiv 13 \cdot 3.$$

(b) $6x \equiv 5 \pmod{15}$

Answer. Since $\gcd(6, 15) = 3$, but $3 \nmid 5$, so there are no solutions.

(c) $8x \equiv 6 \pmod{14}$

Answer. Since $\gcd(8, 14) = 2$ and $2|6$, there are 2 answers. First, $8 * 13 = \equiv_{14} 8 * (-1) \equiv_{14} 6$, so one solution is $\boxed{x = 13}$. Then the other solution is $x = 13 - 14/2 = \boxed{6}$.

(d) $66x \equiv 100 \pmod{121}$

Answer. Since $\gcd(66, 121) = 11$ and $11 \nmid 100$, there are no solutions.

(e) $21x \equiv 14 \pmod{91}$

Answer. Since $\gcd(21, 91) = 7$ and $7 \mid 14$, there are 7 solutions. First, since

$$21 * 87 \equiv_{91} 21 * (-4) = -84 \equiv_{91} 14,$$

we have $x = 87$ is one answer. The other 6 are

$$87 - i(91/7), \qquad \text{for } i = 1, \ldots, 6.$$

(f) $72x \equiv 47 \pmod{200}$

Answer. Since $\gcd(72, 200) = 8$ and $8 \nmid 47$, there are no solutions.

(g) $4183x \equiv 5781 \pmod{15087}$

Answer. Since $\gcd(4183, 15087) = 47$ and $47 \nmid 5781$, there are 47 solutions. First, we use the Euclidean algorithm to solve for u and v such that $4183u + 15087v = 47$:

$$\begin{aligned}
15087 &= 4183 * 3 + 2538,\\
4183 &= 2538 * 1 + 1645,\\
2538 &= 1645 * 1 + 893,\\
1645 &= 893 * 1 + 752,\\
893 &= 752 * 1 + 141,\\
752 &= 141 * 5 + 47;
\end{aligned}$$

so

$$\begin{aligned}
47 = 752 - 141 * 5 &= (1645 - 893 * 1) - (893 - 752 * 1) * 5\\
&= 1645 + (-6) * 893 + 5 * 752\\
&= (4183 - 2538 * 1) + (-6)(2538 - 1645 * 1) + 5 * (1645 - 893 * 1)\\
&= 4183 + (-7) * 2538 + 11 * 1645 + (-5) * 893\\
&= 4183 + (-7) * (15087 - 4183 * 3) + 11 * (4183 - 2538 * 1) + (-5) * (2538 - 1645 * 1)\\
&= 33 * 4183 + (-7) * 15087 + (-16) * 2538 + 5 * 1645\\
&= 33 * 4183 + (-7) * 15087 + (-16) * (15087 - 4183 * 3) + 5 * (4183 - 2538 * 1)\\
&= 86 * 4183 + (-23) * 15087 + (-5) * 2538\\
&= 86 * 4183 + (-23) * 15087 + (-5) * (15087 - 4183 * 3)\\
&= 101 * 4183 + (-28) * 15087.
\end{aligned}$$

Therefore one solution is $x = 101$. The others are

$$101 + i(15087/47), \qquad \text{for } i = 1, \ldots, 46.$$

(h) $1537x \equiv 2863 \pmod{6731}$

Answer. Since $\gcd(1537, 6731) = 53$ and $53 \nmid 2863$, there are no solutions.

Exercise 19. (a) Show that $a \in \mathbb{Z}_{>0}$ is divisible by 4 if and only if its last two digits are divisible by 4. [Hint: consider an equivalence modulo 100.]

Proof. The last two digits of a are by definition the remainder r of a modulo 100:

$$a = 100 * q + r, \quad 0 \leq r < 100.$$

That's equivalent to $r = a - 100 * q$. So since $4|100$, we have

$$4|a \text{ if and only if } 4|a - 100q = r.$$

□

(b) The number $a \in \mathbb{Z}_{>0}$ is divisible by 3 if and only if the sum of its digits is divisible by 3. [Hint: Express a number as integral combination of powers of 10, and reduce modulo 3.]

Proof. We can express a uniquely as a linear combination of powers of 10:

$$a = a_0 + a_1 * 10 + a_2 * 10^2 + \cdots + a_\ell * 10^\ell, \quad \text{with } a_\ell \neq 0.$$

So since $10 \equiv_3 1$, we have $10^k \equiv_3 1^k = 1$ for all k. So

$$a \equiv_3 a_0 + a_1 * 1 + a_2 * 1 + \cdots + a_\ell * 1 = a_0 + a_1 + a_2 + \cdots + a_\ell.$$

□

(c) The number $a \in \mathbb{Z}_{>0}$ is divisible by 9 if and only if the sum of its digits is divisible by 9. [Hint: Express a number as integral combination of powers of 10, and reduce modulo 9.]

Proof. Again, we can express a uniquely as a linear combination of powers of 10:

$$a = a_0 + a_1 * 10 + a_2 * 10^2 + \cdots + a_\ell * 10^\ell, \quad \text{with } a_\ell \neq 0.$$

So since $10 \equiv_9 1$, we have $10^k \equiv_9 1^k = 1$ for all k. So

$$a \equiv_9 a_0 + a_1 * 1 + a_2 * 1 + \cdots + a_\ell * 1 = a_0 + a_1 + a_2 + \cdots + a_\ell.$$

□

Exercise 20.

(a) Use a computer to compute a maximal set of (non-congruent) solutions to the following.

(i) $x^2 \equiv 1 \pmod 8$

Answer. $x = 1, 3, 5, 7$ (see speadsheet).

(ii) $x^2 \equiv 2 \pmod 7$ *Answer.* $x = 3, 4$ (see speadsheet).

(iii) $x^2 \equiv 3 \pmod 7$ *Answer.* No solutions.

(iv) $x^4 + 5x^3 + 4x^2 - 6x = 4 \equiv 0 \pmod{11}$ *Answer.* $x = 1, 9$ (see speadsheet).

(b) For $x^2 \equiv 1 \pmod 8$, you should have gotten more than 2 solutions. Note that these are all solutions to $x^2 - 1 \equiv 0 \pmod 8$. Why isn't this a contradiction to the Polynomial Roots Mod p Theorem?

Answer. 8 is not prime.

(c) Let p and q be distinct primes. What is the maximum number of possible non-congruent solutions to a congruence of the form $x^2 - a \equiv 0 \pmod{pq}$.

Proof. The maximum is four solutions. Suppose that $r_1, \ldots, r_5$ are five distinct solutions. Reducing modulo p, we see that they are solutions to $x^2 - a \equiv 0 \pmod p$. This last congruence has at most two solutions, since p is prime, say s_1 and s_2. Each of $r_1, \ldots, r_5$ must be congruent modulo p to one of s_1 and s_2, so since there are five r_i values and only two s_j values, it follows that at least three of the r_is are the same modulo p. Relabeling, we may assume that $r_1 \equiv_p r_2 \equiv_p r_3$. Next reducing modulo q, we know that $x^2 - a \equiv_q 0$ has at most two solutions, say t_1 and t_2. So the three r_is are each congruent to one of the two t_js, so at least two of the r_is are congruent modulo q. Again relableing, we may assume that $r_1 \equiv r_2 \pmod q$. Thus r_1 and r_2 are congruent both modulo p and modulo q, so they are congruent modulo pq, contradicting the assumption that they are distinct modulo pq. Hence there cannot be five solutions. □

Exercise 21. Use Fermat's Little Theorem to do the following without the use of a computer (show your work!).

(a) Find the least residue of $9^{794} \pmod{73}$.

Answer. Since 73 is prime and $73 \nmid 9$, we have $9^{72} \equiv 1 \pmod{73}$. So since $794 \equiv 2 \pmod{72}$, we have

$$9^{794} \equiv_{73} 9^2 = 81 \equiv_{73} 8.$$

(b) Solve $x^{86} \equiv 6 \pmod{29}$.

Answer. Since 6 is relatively prime to 29, we have $x^{86} \equiv 6 \pmod{29}$ implies x is relatively prime to 29. So $x^{28} \equiv 1 \pmod{29}$. So since $86 \equiv 2 \pmod{28}$, we have $6 \equiv_{29} x^{86} \equiv_{29} x^2$, which has solutions $x = 8$ and 21.

(c) Solve $x^{39} \equiv 3 \pmod{13}$.

Answer. Since 3 is relatively prime to 13, we have $x^{39} \equiv 3 \pmod{13}$ implies x is relatively prime to 13. So $x^{12} \equiv 1 \pmod{13}$. So since $39 \equiv 3 \pmod{12}$, we have $3 \equiv_{13} x^{86} \equiv_{13} x^3$. But this has no solutions.

Exercise 22. Recall the quantity $(p-1)! \pmod{p}$ appeared in our proof of Fermats Little Theorem (without actually having to compute it).

(a) Use a computer to calculate $(p-1)! \pmod{p}$ for primes p up to 13.

Answer.

p	2	3	5	7	11	13
$(p-1)! \pmod{p}$	1	-1	-1	-1	-1	-1

(b) Make a conjecture for what $(p-1)! \pmod{p}$ is in general, and prove it.
[Hint: Do a few examples by hand – say for $p = 2, 3$, and 5, and try to discover why $(p-1)! \pmod{p}$ has the value it does. Then generalize your observation to prove the formula for all values of p.]

Answer. We have $(p-1)! \equiv -1 \pmod{p}$, unless $p = 2$ (in which case it is equivalent to 1). This is because every number $1 \leq a \leq p-1$ has a multiplicative inverse (something that you can multiply them by to get 1 mod p). For $p \geq 3$, there are exactly two values that are their own inverses (i.e. solutions to $a^2 \equiv_p 1$), which are 1 and $p - 1 \equiv_p -1$. So all the other numbers pair up to multiply by 1. For example,

$$1 * 2 * 3 * 4 * 5 * 6 = 1 * (2 * 4) * (3 * 5) * 6 \equiv_7 1 * 1 * 1 * (-1) = -1.$$

So

$$(p-1)! = 1 * 2 * 3 * \cdots * (p-2) * (p-1) \equiv_p 1 * 1 * \cdots * 1 * (-1) = -1.$$

Otherwise, for $p = 2$, we have $(p-1)! = 1! = 1$.

(c) Compute the value of $(m-1)! \pmod{m}$ for some small values of m that are not prime ($m = 4, 6, \ldots$). Do you find the same pattern as you found for primes? Do you see any pattern?

Answer. For most values, $(m-1)! \equiv 0 \pmod{m}$. This is because if m is composite, and not a prime power, there are a and b less than m that are relatively prime that satisfy $ab = m$. So $m = ab|(m-1)!$. If m is a prime power, with $m = p^k$, then p^{k-1} is one of the factors of $(p^k - 1)!$; and as long as $p > 2$ or $k > 2$, then there is a distinct factor in $(p^k - 1)!$ that is a multiple of p. So $p * p^{k-1} | (p^k - 1)!$. The only exception, therefore, is $m = 4$, in which case $(m-1)! = 3! = 6 \equiv_4 2$.