CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Alistair Sinclair and Yun Song

HW 4

1 Modular Arithmetic Solutions

Find all solutions (modulo the corresponding modulus) to the following equations. Prove that there are no other solutions (in a modular setting) to each equation.

(a) $2x \equiv 5 \pmod{15}$

(b) $2x \equiv 5 \pmod{16}$

(c) $5x \equiv 10 \pmod{25}$

Solution:

(a) Since 2 has an inverse modulo 15, this equation will have exactly one solution. We can get this solution by multiplying both sides by $2^{-1} \pmod{15}$, which is 8. This gives us that $x \equiv 40 \equiv 10 \pmod{15}$.

(b) Our trick from the last part doesn't work any more, since 2 is not relatively prime to 16, and thus doesn't have a multiplicative inverse mod 16. Indeed, this equation has no solutions at all, since the left side will always be even and the right side will always be odd. More formally, we know that $2x \equiv 5 \pmod{16}$ is equivalent to $2x + 16k = 5$ for some $k \in \mathbb{Z}$. We can factor out a two from the left hand side, showing that it is divisible by 2, so there is no choice of x and k that will make the equality hold.

(c) Again, we have that the coefficient on x does not have a multiplicative inverse in our chosen modulus. However, unlike the previous part, we can still find solutions to this equation. We can see by inspection that $x = 2$ will be one possible solution. Furthermore, if x is a solution to this equation, $x + 5$ will be as well, since $5(x+5) = 5x + 25 \equiv 5x \pmod{25}$. This tells us that $x = 7$, $x = 12$, $x = 17$, and $x = 22$ are also solutions to this equation.

We now just have to show that these are the only five solutions to this equation modulo 25. Suppose we have some solution x to the equation. This means that $5x \equiv 10 \pmod{25}$, or equivalently, that $5x + 25k = 10$ for some $k \in \mathbb{Z}$. This is now an equation over the real numbers, so we can divide the whole thing by 5, giving us that $x + 5k = 2$. But now that's just definitionally saying that $x \equiv 2 \pmod{5}$. Thus, we have that all solutions to this equation must be equivalent to 2 modulo 5–and the only numbers modulo 25 that satisfy this condition are 2, 7, 12, 17, and 22. This tells us that indeed, these five numbers are the only possible values for x.

2 Euclid's Algorithm

(a) Use Euclid's algorithm from lecture to compute the greatest common divisor of 527 and 323. List the values of x and y of all recursive calls.

(b) Use extended Euclid's algorithm from lecture to compute the multiplicative inverse of 5 mod 27. List the values of x and y and the returned values of all recursive calls.

(c) Find $x \pmod{27}$ if $5x + 26 \equiv 3 \pmod{27}$. You can use the result computed in (b).

(d) Assume a, b, and c are integers and $c > 0$. Prove or disprove: If a has no multiplicative inverse mod c, then $ax \equiv b \pmod{c}$ has no solution.

Solution:

(a) The values of x and y of all recursive calls are (you can get full credits without the column of x mod y):

Function Calls	(x,y)	x mod y
#1	$(527,323)$	204
#2	$(323,204)$	119
#3	$(204,119)$	85
#4	$(119,85)$	34
#5	$(85,34)$	17
#6	$(34,17)$	0
#7	$(17,0)$	—

Therefore, $\gcd(527,323) = 17$.

(b) To compute the multiplicative inverse of 5 mod 27, we first call `extended-gcd(27,5)`. Note that `(x div y)` in the pseudocode means $\lfloor x/y \rfloor$. The values of x and y of all recursive calls are (you can get full credits without the columns of x div y and x mod y):

Function Calls	(x,y)	x div y	x mod y
#1	$(27,5)$	5	2
#2	$(5,2)$	2	1
#3	$(2,1)$	2	0
#4	$(1,0)$	—	—

The returned values of all recursive calls are:

Function Calls	(d,a,b)	Returned Values
#4	—	$(1,1,0)$
#3	$(1,1,0)$	$(1,0,1)$
#2	$(1,0,1)$	$(1,1,-2)$
#1	$(1,1,-2)$	$(1,-2,11)$

Therefore, we get $1 = (-2) \times 27 + 11 \times 5$ and

$$1 = (-2) \times 27 + 11 \times 5 \equiv 11 \times 5 \pmod{27},$$

so the multiplicative inverse of 5 mod 27 is 11.

(c)

$$\begin{aligned} 5x + 26 \equiv 3 \pmod{27} &\Rightarrow 5x \equiv 3 - 26 \pmod{27} \\ &\Rightarrow 5x \equiv -23 \pmod{27} \\ &\Rightarrow 5x \equiv 4 \pmod{27} \\ &\Rightarrow 11 \times 5x \equiv 11 \times 4 \pmod{27} \\ &\Rightarrow x \equiv 44 \pmod{27} \\ &\Rightarrow x \equiv 17 \pmod{27}. \end{aligned}$$

(d) False. We can have a counterexample: $a = 3$, $b = 6$, and $c = 12$, so a has no multiplicative inverse mod c (because $a = 3$ and $c = 12$ are not relatively prime). However, $3x \equiv 6 \pmod{12}$ has solutions $x = 2, 6, 10$ mod 12.

3 Modular Exponentiation

Compute the following:

(a) $13^{2018} \pmod{12}$

(b) $8^{11111} \pmod{9}$

(c) $7^{256} \pmod{11}$

(d) $3^{160} \pmod{23}$

Solution:

(a) 13 is always 1 mod 12, so 13 to any power mod 12 is 1.

(b) 8 is its own inverse mod 9, therefore, if 8 is raised to an odd power, the number will be 8 mod 9. So the answer is 8.

Also notice that $8 \equiv -1 \pmod{9}$ so $8^{11111} \equiv (-1)^{11111} \equiv -1 \equiv 8 \pmod{9}$. In general, $m - 1 \equiv -1 \pmod{m}$, so $m - 1$ is always its own inverse. This is a useful trick so you can avoid computing the inverse of $m - 1$ by hand. You can also check that $(m-1)^2 \equiv m^2 - 2m + 1 \equiv 1 \pmod{m}$, which is another proof that $m - 1$ is its own inverse modulo m.

(c) We can use repeated squaring for this question.

$7^2 \equiv 5 \pmod{11}$
$7^4 \equiv (7^2)^2 \equiv 5^2 \equiv 3 \pmod{11}$
$7^8 \equiv (7^4)^2 \equiv 3^2 \equiv 9 \pmod{11}$
$7^{16} \equiv (7^8)^2 \equiv 9^2 \equiv 4 \pmod{11}$
$7^{32} \equiv (7^{16})^2 \equiv 4^2 \equiv 5 \pmod{11}$
$7^{64} \equiv (7^{32})^2 \equiv 5^2 \equiv 3 \pmod{11}$
$7^{128} \equiv (7^{64})^2 \equiv 3^2 \equiv 9 \pmod{11}$
$7^{256} \equiv (7^{128})^2 \equiv 9^2 \equiv 4 \pmod{11}$

(d) We can notice that $160 = 128 + 32$, the sum of two powers of two. Then, like the previous part, we can use repeated squaring to compute this problem.

$3^2 \equiv 9 \pmod{23}$
$3^4 \equiv (3^2)^2 \equiv 9^2 \equiv 12 \pmod{23}$
$3^8 \equiv (3^4)^2 \equiv 12^2 \equiv 6 \pmod{23}$
$3^{16} \equiv (3^8)^2 \equiv 6^2 \equiv 13 \pmod{23}$
$3^{32} \equiv (3^{16})^2 \equiv 13^2 \equiv 8 \pmod{23}$
$3^{64} \equiv (3^{32})^2 \equiv 8^2 \equiv 18 \pmod{23}$
$3^{128} \equiv (3^{64})^2 \equiv 18^2 \equiv 2 \pmod{23}$
$3^{160} \equiv (3^{128})(3^{32}) \equiv (2)(8) \equiv 16 \pmod{23}$

4 Euler's Totient Function

Euler's totient function is defined as follows:

$$\phi(n) = |\{i : 1 \le i \le n, \texttt{gcd}(n,i) = 1\}|$$

In other words, $\phi(n)$ is the total number of positive integers less than or equal to n which are relatively prime to it. Here is a property of Euler's totient function that you can use without proof: For m,n such that $\texttt{gcd}(m,n) = 1$, $\phi(mn) = \phi(m) \cdot \phi(n)$.

(a) Let p be a prime number. What is $\phi(p)$?

(b) Let p be a prime number and k be some positive integer. What is $\phi(p^k)$?

(c) Let p be a prime number and a be a positive integer smaller than p. What is $a^{\phi(p)} \pmod{p}$? *(Hint: use Fermat's Little Theorem.)*

(d) Let b be a positive integer whose prime factors are $p_1, p_2, \dots, p_k$. We can write $b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$.

Show that for any a relatively prime to b, the following holds:

$$\forall i \in \{1, 2, \dots, k\},\ a^{\phi(b)} \equiv 1 \pmod{p_i}$$

Solution:

(a) Since p is prime, all the numbers from 1 to $p-1$ are relatively prime to p.

So, $\phi(p) = p - 1$.

(b) The only positive integers less than p^k which are not relatively prime to p^k are multiples of p.

Why is this true? This is so because the only possible prime factor which can be shared with p^k is p. Hence, if any number is not relatively prime to p^k, it has to have a prime factor of p which means that it is a multiple of p.

The multiples of p which are $\leq p^k$ are $1 \cdot p, 2 \cdot p, \dots, p^{k-1} \cdot p$. There are p^{k-1} of these.

The total number of positive integers less than or equal to p^k is p^k.

So $\phi(p^k) = p^k - p^{k-1} = p^{k-1} \cdot (p-1)$.

(c) From Fermat's Little Theorem, and part (a),

$a^{\phi(p)} \equiv a^{p-1} \equiv 1 \pmod{p}$

(d) From the property of the totient function and part (b):

$$\begin{aligned}
\phi(b) &= \phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}) \\
&= \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \dots \phi(p_k^{\alpha_k}) \\
&= p_1^{\alpha_1 - 1}(p_1 - 1) \cdot p_2^{\alpha_2 - 1}(p_2 - 1) \dots p_k^{\alpha_k - 1}(p_k - 1)
\end{aligned}$$

This shows that, for every p_i, which is a prime factor of b, we can write $\phi(b) = c \cdot (p_i - 1)$, where c is some constant. Since a and b are relatively prime, a is also relatively prime with p_i. From Fermat's Little Theorem:

$a^{\phi(b)} \equiv a^{c \cdot (p_i - 1)} \equiv (a^{(p_i - 1)})^c \equiv 1^c \equiv 1 \mod p_i$

Since we picked p_i arbitrarily from the set of prime factors of b, this holds for all such p_i.

5 FLT Converse

Recall that the FLT states that, given a prime n, $a^{n-1} \equiv 1 \pmod{n}$ *for all* $1 \leq a \leq n-1$. Note that it says nothing about when n is composite.

Can the FLT condition ($a^{n-1} \equiv 1 \mod n$) hold for some or even all a if n is composite? This problem will investigate both possibilities. It turns out that unlike in the prime case, we need to restrict ourselves to looking at a that are relatively prime to n. (Note that if n is prime, then every $a < n$ is relatively prime to n). Because of this restriction, let's define

$$S(n) = \{i : 1 \le i \le n, \texttt{gcd}(n,i) = 1\},$$

so $\mid S \mid$ is the total number of possible choices for a.

(a) Prove that for every a and n that are not relatively prime, FLT condition fails. In other words, for every a and n such that $\texttt{gcd}(n,a) \neq 1$, we have $a^{n-1} \not\equiv 1 \pmod{n}$.

(b) Prove that the FLT condition fails for most choices of a and n. More precisely, show that if we can find a single $a \in S(n)$ such that $a^{n-1} \not\equiv 1 \pmod{n}$, we can find at least $|S(n)|/2$ such a. (Hint: You're almost there if you can show that the set of numbers that fail the FLT condition is at least as large as the set of numbers that pass it. A clever bijection may be useful to compare set sizes.)

The above tells us that if a composite number fails the FLT condition for even one number relatively prime to it, then it fails the condition for most numbers relatively prime to it. However, it doesn't rule out the possibility that some composite number n satisifes the FLT condition entirely: *for all* a relatively prime to n, $a^{n-1} \equiv 1 \mod n$. It turns out such numbers do exist, but they were found through trial-and-error! We will prove one of the conditions on n that make it easy to verify the existence of these numbers.

(c) First, show that if $a \equiv b \mod m_1$ and $a \equiv b \mod m_2$, with $\gcd(m_1, m_2) = 1$, then $a \equiv b \pmod{m_1 m_2}$.

(d) Let $n = p_1 p_2 \cdots p_k$ where p_i are distinct primes and $p_i - 1 \mid n - 1$ for all i. Show that $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in S(n)$

(e) Verify that for all a coprime with 561, $a^{560} \equiv 1 \pmod{561}$.

Solution:

(a) Let $c = \texttt{gcd}(n,a) \neq 1$. Clearly $n > 1$, otherwise we would have $\texttt{gcd}(1,a) = 1$. Suppose on the contrary that $a^{n-1} \equiv 1 \pmod{n}$.

Note that $a^{n-1} \equiv 1 \pmod{n}$ if and only if there exists $k \in \mathbb{N}$, $a^{n-1} - nk = 1$. Since $c \mid n$ and $c \mid a$, we must have $c \mid (a^{n-1} - nk)$ for every $k \in \mathbb{N}$. On the other hand $c \neq 1$, thus $c \nmid 1$, contradicting the fact that $a^{n-1} - nk = 1$. As a result, $a^{n-1} - nk \neq 1$ for every $k \in \mathbb{N}$, and thus $a^{n-1} \equiv 1 \pmod{n}$.

(b) The key to this argument is that we've already found one a that breaks the FLT condition. Let N_f be the set of integers coprime with n that fail the FLT condition, and N_p be the set of integers coprime with n that pass it. Note that $N_f \cup N_p = S(n)$, so $\mid N_f \mid + \mid N_p \mid = \mid S(n) \mid$. Therefore, our goal is to show that $|N_f| \geq |N_p|$, so that $|N_p| < \frac{S(n)}{2}$ immediately follows.

Assume there's another number b for which $b^{n-1} \equiv 1 \mod n$, i.e. $b \in N_p$. Consider $(a \cdot b)^{n-1} = a^{n-1}b^{n-1} = a^{n-1} \not\equiv 1 \mod n$, by assumption. So, given any b that satisfies the FLT condition, we can construct a number ab that breaks it! But is $ab \mod n$ unique? Yes, because $ax \mod n$ is a bijection, since $\gcd(a,n) = 1$. So for every $b \in N_p$, $ab \in N_f$, and $|N_p| \leq |N_f|$.

(c) This is a specialized version of the CRT where we can combine the moduli without calculating inverses. If $a = b \mod m_1$, then $a = km_1 + b$ for some k in $\mathbb{Z}$. If $a = b \mod m_2$, then $a = lm_2 + b$ for some $l \in \mathbb{Z}$. We want to relate the two moduli, so rewrite this as $a - b = lm_2$ and $a - b = km_1$, or $lm_2 = km_1$. Since m_1 and m_2 are coprime, $m_1 \mid l \implies l = dm_1$ for some $d \in \mathbb{Z}$. Substituting back in, we find $lm_2 = dm_1m_2 \implies a - b = dm_1m_2$. So, $a = b \mod m_1m_2$.

(d) Since p_i are prime, we know that $a^{p_i-1} = 1 \mod p_i$. Since $p_i - 1 \mid n-1$, $a^{n-1} = a^{j(p_i-1)} = (a^{p_i-1})^j = 1 \mod p_i$. This holds for all a coprime with p_i. Thus, if we restrict ourselves to a that are coprime with all p_i, we have a set of k equations $a^{n-1} = 1 \mod p_i$. By the last part, we can conclude $a^{n-1} = 1 \mod n$, for any a that is coprime with all of the p_i. This condition is the same as a coprime with n, so we've shown n passes the FLT condition for “primality".

(e) $561 = 3 \times 11 \times 17$, and $2 \mid 560$, $10 \mid 560$, and $16 \mid 560$. By the above condition, 561 passes the FLT test.