6.042/18.062J Mathematics for Computer Science — September 16, 2014
Tom Leighton and Ankur Moitra

Problem Set 3 Solutions

Due: Monday, September 22

Reading Assignment: Sections 4.0-4.3, 4.5-4.8

Problem 1. [16 points] Warmup Exercises

For the following parts, a correct numerical answer will only earn credit if accompanied by it's derivation. Show your work.

(a) [4 pts] Use the Pulverizer to find integers s and t such that $139s + 61t = \gcd(139, 61)$.

Solution.

x	y	$\text{rem}\,(x, y)$	$=$	$x - q \cdot y$
139	61	17	$=$	$139 - 2 \cdot 61$
61	17	10	$=$	$61 - 3 \cdot 17$
			$=$	$61 - 3 \cdot (139 - 2 \cdot 61)$
			$=$	$-3 \cdot 139 + 7 \cdot 61$
17	10	7	$=$	$17 - 10$
			$=$	$(139 - 2 \cdot 61) - (-3 \cdot 139 + 7 \cdot 61)$
			$=$	$4 \cdot 139 - 9 \cdot 61$
10	7	3	$=$	$10 - 7$
			$=$	$(-3 \cdot 139 + 7 \cdot 61) - (4 \cdot 139 - 9 \cdot 61)$
			$=$	$-7 \cdot 139 + 16 \cdot 61$
7	3	1	$=$	$7 - 2 \cdot 3$
			$=$	$(4 \cdot 139 - 9 \cdot 61) - 2 \cdot (-7 \cdot 139 + 16 \cdot 61)$
			$=$	$\boxed{18 \cdot 139 - 41 \cdot 61}$
3	1	0		

Exam tip: *Each time rem(x, y) is calculated, substitutions are immediately made to then express it as a linear combination of 139 and 61 (using the remainders calculated on previous lines). Simplifying at each step leads to a much faster computation of s and t.* ■

(b) [4 pts] Use the previous part to find the inverse of 61 modulo 139 in the range $\{1, \ldots, 138\}$.

Solution. 98

From part (a), $1 = 18 \cdot 139 - 41 \cdot 61$ and so $1 \equiv -41 \cdot 61 \pmod{139}$. Therefore -41 is *an* inverse of 61. However, it is not the *unique* inverse of 61 in the range $\{1, \ldots, 139\}$, which is given by $\operatorname{rem}(-41, 139) = 98$. One can easily check this by multiplication. ■

(c) [4 pts] Use Euler's theorem to find the inverse of 19 modulo 37 in the range $\{1, \ldots, 30\}$.

Solution. 2

Since 37 is prime, Euler's theorem implies $19^{37-2} \cdot 19 \equiv 1 \pmod{37}$ and so $\operatorname{rem}(19^{37-2}, 37)$ is the inverse of 19 in the range $\{1, \ldots, 36\}$. Using the method of repeated squaring,

$$\begin{aligned}
19^2 &= 361 \\
&= 9 \cdot 37 + 28 \\
&\equiv 28 \\[1em]
19^4 &\equiv 28^2 \\
&= 784 \\
&= 21 \cdot 37 + 7 \\
&\equiv 7 \\[1em]
19^8 &\equiv 7^2 \\
&= 49 \\
&= 37 + 12 \\
&\equiv 12 \\[1em]
19^{16} &\equiv 12^2 \\
&= 144 \\
&= 3 \cdot 37 + 33 \\
&\equiv 33 \\[1em]
19^{32} &\equiv 33^2 \\
&= 1089 \\
&= 29 \cdot 37 + 16 \\
&\equiv 16 \\[1em]
19^{35} &= 19^{32} \cdot 19^2 \cdot 19^1 \\
&\equiv 16 \cdot 28 \cdot 19 \\
&\equiv \boxed{2}
\end{aligned}$$

where the modulus for each of the congruences is 37. ■

(d) [4 pts] Find the remainder of 38^{82248} divided by 83. (*Hint: Euler's theorem.*)

Solution. 33

Since $38 = 2 \cdot 19$ and 83 are relatively prime, Euler's theroem implies that $38^{\phi(83)} \equiv 1 \pmod{83}$ where

$$\phi(83) = 82$$

Now, notice that $82248 = 82 \cdot 1003 + 2$. But then, this implies that

$$\begin{aligned} 38^{82248} &= 38^2 \cdot 38^{1003 \cdot 82} \\ &\equiv 38^2 \cdot 1^{1003} \pmod{83} && \text{(by Euler's Theorem)} \\ &= 1444 \\ &\equiv 33 \pmod{83} \end{aligned}$$

■

Problem 2. [16 points]

Prove the following statements, assuming all numbers are positive integers.

(a) [4 pts] If $a \mid b$, then $\forall c,\ a \mid bc$

Solution. If $a \mid b$, then there is some positive integer k such that $b = ak$. But then, $bc = akc = a(kc)$, which is a multiple of a. ■

(b) [4 pts] If $a \mid b$ and $a \mid c$, then $a \mid sb + tc$.

Solution. If $a \mid b$, then there is some positive integer j such that $b = aj$. Similarly, there is some positive integer k such that $c = ak$. But then, we can rewrite the right side as $s(aj) + t(ak)$. But we can rewrite this as $a(js) + a(kt) = a(js + kt)$, which is a multiple of a. ■

(c) [4 pts] $\forall c,\ a \mid b \Leftrightarrow ca \mid cb$

Solution. If $a \mid b$, then there is some positive integer k such that $b = ak$. But then, we can rewrite $cb = c(ak) = ca(k)$, from which it follows that cb is a multiple of ca. So the implication is true. Conversely, if $ca \mid cb$ then there is some positive integer k such that $cb = cak$. We can cancel c from both sides to conclude that $a \mid b$. ■

(d) [4 pts] $\gcd(ka, kb) = k \gcd(a, b)$

Solution. Let s, t be coefficients so that $s(ka) + t(kb) = \gcd(ka, kb)$. We can factor out the k so that $\gcd(ka, kb) = k(sa + tb)$. We now argue that $sa + tb = \gcd(a, b)$. Suppose it were not. Then, there is some smaller positive linear combination of a, b with coefficients s' and t' so that $s'a + t'b = \gcd(a, b)$. But then, if we multiply this by k, we find that $0 < ks'a + kt'b = s'(ka) + t'(kb) < s(ka) + t(kb) = \gcd(ka, kb)$. This is a contradiction with the definition of the gcd, so $sa + tb = \gcd(a, b)$, and we can conclude that $\gcd(ka, kb) = k \gcd(a, b)$. ■

Problem 3. [20 points] In this problem, we will investigate numbers which are squares modulo a prime number p.

(a) [5 pts] An integer n is a square modulo p if there exists another integer x such that $n \equiv x^2 \pmod{p}$. Prove that $x^2 \equiv y^2 \pmod{p}$ if and only if $x \equiv y \pmod{p}$ or $x \equiv -y \pmod{p}$. (*Hint:* $x^2 - y^2 = (x+y)(x-y)$)

Solution. $x^2 \equiv y^2 \pmod{p}$ iff $p \mid x^2 - y^2$. But $x^2 - y^2 = (x-y)(x+y)$, and since p is a prime, this happens iff either $p \mid x - y$ or $p \mid x + y$, which is iff $x \equiv y \pmod{p}$ or $x \equiv -y \pmod{p}$. ■

(b) [5 pts] There is a simple test we can perform to see if a number n is a square modulo p. It states that

Theorem 1 (Euler's Criterion)**.** *:*

1. *If n is a square modulo p then $n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.*
2. *If n is not a square modulo p then $n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.*

Prove the first part of Euler's Criterion. (*Hint: Use Fermat's theorem.*)

Solution. If n is a square modulo p, then there exists an x such that $x^2 \equiv n(modp)$. Consequently,

$$a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$$

by Fermat's theorem. ■

(c) [10 pts] Assume that $p \equiv 3 \pmod{4}$ and $n \equiv x^2 \pmod{p}$. Fine one possible value for x, expressed as a function of n and p. (*Hint: Write p as $p = 4k+3$ and use Euler's Criterion. You might have to multiply two sides of an equation by n at one point.*)

Solution. From Euler's Criterion:

$$n^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

We can write $p = 4k+3$, so $\frac{p-1}{2} = \frac{4k+3-1}{2} = k+1$. As a result, $n^{2k+1} \equiv 1 \pmod{p}$, so $n^{2k+2} \equiv n \pmod{p}$. This can be rewritten as $\left(n^{k+1}\right)^2 \equiv n \pmod{p}$, so

$$n^{k+1} = n^{\frac{p-3}{4}+1}$$

is one possible value of x. ■

Problem 4. [10 points] Prove that for any prime, p, and integer, $k \geq 1$,

$$\phi(p^k) = p^k - p^{k-1},$$

where ϕ is Euler's function. (*Hint: Which numbers between 0 and $p^k - 1$* are *divisible by p? How many are there?*)

Solution. The numbers in the interval from 0 to $p^k - 1$ that are divisible by p are all those of the form mp. For mp to be in the interval, m can take any value from 0 to $p^{k-1} - 1$ and no others, so there are exactly p^{k-1} numbers in the interval that are divisible by p. Now $\phi(p^k)$ equals the number of remaining elements in the interval, namely, $p^k - p^{k-1}$. ■

Problem 5. **[10 points]** Using the RSA encryption system, Pete the publisher generates a private key (d, n) and posts a public key, (e, n), which anyone can use to send encrypted messages to Pete.

RSA has the useful property that these same keys can switch roles: if Pete wants to broadcast an unforgeable "signed" message, he can encrypt his message using his private key as though it was someone's public key. That is, from a plain text $m \in [0, n)$, Pete would broadcast a signed version, $s = \text{rem}\,(m^d, n)$.

Then anyone can decrypt and read Pete's broadcast message by using Pete's public key as though it were their own private key. Readers of Pete's message can be sure the message came from Pete if they believe that the only way to generate such a message is by using the private key which Pete alone knows. (This belief is widely accepted, but not certain.)

(a) [5 pts] Explain exactly what calculation must be performed on s to recover m using the public key (e, n). Explain why the calculation yields the plain text m.

Solution.

$$m = \text{rem}\,(s^e, n)$$

The requirement for RSA decryption, namely that $de \equiv 1 \pmod{(p-1)(q-1)}$, is symmetric in d and e, so reversing their roles allows the private key d to be used to encrypt and the public key e to decrypt. ■

(b) [5 pts] Big Earl notices that the next problem on the 6.042 students homework seems like it could be difficult to solve without guidance (or without showing up to lecture). He decides to send the encrypted, authenticated message 1535 to the students, who can use the public key (7, 7613) to decrypt the message. Each digit of the original message corresponds to a letter of the alphabet found in the following legend:

$$\begin{aligned}
0 &= u\\
1 &= e\\
2 &= o\\
3 &= i\\
4 &= b\\
5 &= s\\
6 &= h\\
7 &= c\\
8 &= x\\
9 &= k
\end{aligned}$$

What is the original message, and to what one-word hint does it correspond?

Solution. The original message is $\text{rem}\,(1535^7, 7613) = 4229$ which corresponds to the word “book”. ■

Problem 6. [10 points] The Lucas series is defined by:

$$\begin{aligned} L_1 &= 2 \\ L_2 &= 1 \\ L_n &= L_{n-1} + L_{n-2} \text{ for } n \geq 3 \end{aligned}$$

Prove that L_n and L_{n+1} are relatively prime.

Solution. This is similar to a problem we had during recitation with Fibonacci numbers. We use induction on n. Let $P(n)$ be the proposition that L_n and L_{n+1} are relatively prime.

Base Case: $P(1)$ is true because $L_1 = 2$ and $L_2 = 1$ are relatively prime.

Inductive step: We show that, for all $n \geq 1$, $P(n)$ implies $P(n+1)$. So, fix some $n \geq 1$ and assume that $P(n)$ is true, that is, L_n and L_{n+1} are relatively prime. We will show that L_{n+1} and L_{n+2} are relatively prime as well. We will do this by contradiction.

Suppose L_{n+1} and L_{n+2} are not relatively prime. Then they have a common divisor $d > 1$. But then d also divides the linear combination $L_{n+2}L_{n+1}$, which actually equals L_n . Hence, $d > 1$ divides both L_n and L_{n+1} . Which implies L_n , L_{n+1} are not relatively prime, a contradiction to the inductive hypothesis.

Therefore, L_{n+1} and L_{n+2} are relatively prime. That is, $P(n+1)$ is true.

The theorem follows by induction. ■

Problem 7. [10 points] In this problem, we will investigate systems of linear congruence equations.

(a) [5 pts] Prove that for integers a and b,

$$x = rem(bsm + atn, mn)$$

is the unique solution in the range $0, 1, \ldots, mn-1$ to the system of equations

$$\begin{aligned} x &\equiv a \pmod{m} \quad (1) \\ x &\equiv b \pmod{n} \quad (2) \\ & \quad (3) \end{aligned}$$

(Hint: There are two steps to this proof: (i) show that it is a solution, (ii) show that this solution is unique.)

Solution. By the definition of rem, there exists an integer v such that

$$x = bsm + atn + vmn \in \{0, 1, \ldots, mn - 1\}$$

Collecting multiples of m and applying $sm + tn = 1$,

$$\begin{aligned} x &= atn + (bs + vn)m \\ &\equiv atn \pmod{m} \\ &= a(1 - sm) \\ &\equiv a \pmod{m} \end{aligned}$$

Similarly,

$$\begin{aligned} x &= bsm + (at + vm)n \\ &\equiv bsm \pmod{n} \\ &= b(1 - tn) \\ &\equiv b \pmod{n} \end{aligned}$$

Therefore it is a solution.

Next suppose that x, x' both satisfy congruences. Taking the differences we see that

$$x - x' \equiv 0 \pmod{m} \text{ and } x - x' \equiv 0 \pmod{n}$$

So by definition, both m and n divide $x - x'$, and since m and n are relatively prime, this implies $mn|(x - x')$. But if x and x' are both in the range 0 to $mn - 1$, then $mn > |x - x'|$, so it must be that $x = x'$, as required. ■

(b) [5 pts] Next we will investigate the general case.

Theorem 2 (Chinese Remainder Theorem)**.** *Suppose that $n_1, n_2, ..., n_k$ are coprime. Then the following system of equations*

$$x \equiv a_i \pmod{n_i}, \qquad i = 1, \cdots, k$$

has a solution x, and moreover all such solutions are congruent modulo $N = n_1 \ldots n_k$

We will construct an explicit solution. For each i, the integers n_i and $\frac{N}{n_i}$ are coprime and we can use the Pulverizer to find $r_i, s_i \in \mathbb{Z}$ such that $r_i n_i - \frac{s_i N}{n_i} = 1$.

Prove that $x = \sum_{i=1}^{k} a_i \frac{s_i N}{n_i}$ is a solution.

Solution. Let $e_i = \frac{s_i N}{n_i}$.

$$\begin{aligned} r_i n_i + e_i &= 1 \\ e_i &\equiv 1 \pmod{n_i} \end{aligned}$$

And $e_i = \frac{s_i N}{n_i} = \frac{s_i n_1 \ldots n_k}{n_i}$. So n_j for $j \neq i$ divides e_i

To summarize

$$e_i \equiv \begin{cases} 1 \pmod{n_i} \\ 0 \pmod{n_j} & j \neq i \end{cases}$$

Because of the basic properties of modular arithmetic, x satisfies all of the congruence equations. ■