

NAME: Solutions

Math 52 Practice for Test II on Friday, April 10, 2009

Explain each step along the way in order to fully demonstrate your knowledge

1. EXTENDED EUCLIDEAN ALGORITHM

- a. Use the Euclidean Algorithm to find integer values of x and y such that $23x + 57y = 1$. Show your work.

$$\begin{aligned} (57) &= 2(23) + (11) && \text{The Euclidean algorithm consists of} \\ (23) &= 2(11) + (1) && \text{repeating the Division algorithm.} \end{aligned}$$

$$\begin{aligned} \text{So } (1) &= (23) - 2(11) \quad (\text{back-substitution}) \quad (\text{This is the extended} \\ &= (23) - 2[(57) - 2(23)] && \text{Euclidean algorithm)} \\ &= 5(23) - 2(57) \end{aligned}$$

$$\text{So } \boxed{x=5, y=-2}$$

- b. What is the GCD of 23 and 57?

$\boxed{1}$ found above.

- c. Find $23^{-1} \pmod{57}$.

The definition of $b = a^{-1} \pmod{m}$ is $ba \equiv 1 \pmod{m}$.

Since $1 = 5 \cdot 23 - 2(57)$ we see

$$1 \equiv 5 \cdot 23 \pmod{57}$$

$$\boxed{\text{Thus } 5 = 23^{-1} \pmod{57}.}$$

- d. Solve for z such that $23z \equiv 3 \pmod{57}$.

Since we have found $5 = 23^{-1} \pmod{57}$, we can multiply both sides of the congruence by 5 and use the rules of modular arithmetic.

$$z \equiv 1 \cdot z \equiv (5 \cdot 23) \cdot z \equiv 5 \cdot (23z) \equiv 5 \cdot 3 \equiv 15 \pmod{57}$$

$$\text{So } \boxed{z \equiv 15 \pmod{57}}$$

- e. Name 3 integers between 1 and 56 that do not have inverses mod 57.

They will not have inverses if they have a factor in common with $57 = 3 \cdot 19$.

So integers without inverses are $\boxed{3, 6, 9, 12, 15, 18, 19, \dots}$

- f. The extended Euclidean algorithm leads to the proof that the greatest common divisor of a and b , can be written as $(a, b) = ax + by$ for some integers x and y . State one or more facts that can be proved as a consequence of this explicit expression for the greatest common divisor.

This is used to prove: 1) $(a, b) = 1$ and $a | bc \Rightarrow a | c$

2) a has an inverse mod $m \Leftrightarrow (a, m) = 1$

3) The Chinese Remainder Thm: The solution to $A \equiv a \pmod{m}$ and $A \equiv b \pmod{n}$ with $1 \leq A \leq mn$ and $(m, n) = 1$ is $A \equiv ax + by \pmod{mn}$

2. MODULAR ARITHMETIC

- a. List two other statements which are equivalent to the statement that $a \equiv b \pmod{m}$.

$$a = b + km \text{ for some } k \in \mathbb{Z}$$

$$m \mid a - b$$

$$\frac{a-b}{m} \in \mathbb{Z}$$

$$a \pmod{m} = b \pmod{m} \quad (\text{definition})$$

- b. Explain why $\mathbb{Z}/p\mathbb{Z}$ is a field when p is a prime number.

If p is prime, its ^{positive} only factors are 1 and p .

So when we take any integer $a < p$, it cannot have a factor of p . The only factor it can have in common with p is 1.

When $(a, p) = 1$, we have proved that a has an inverse mod p . This shows that $1, 2, 3, \dots, p-1$ all have multiplicative inverses mod p . So every elt. except 0 in $\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \dots, p-1\}$ has an inverse. That makes it a field.

- c. What is the definition of $u = a^{-1} \pmod{m}$?

$$ua \equiv 1 \pmod{m}.$$

- d. If u is the inverse of $a \pmod{m}$, and n is a positive integer, show that u^n is the inverse of $a^n \pmod{m}$.

u is inverse of $a \pmod{m}$

$$\Leftrightarrow ua \equiv 1 \pmod{m} \text{ by definition}$$

$$\Rightarrow (ua)^n \equiv 1^n \pmod{m} \text{ by rules of modular arithmetic}$$

$$\Rightarrow u^n a^n \equiv 1 \pmod{m} \text{ Since } (ua)^n = u^n a^n$$

$$\Rightarrow u^n \text{ is the inverse of } a^n \pmod{m}, \text{ by definition.}$$

3. FERMAT'S LITTLE THEOREM

- a. State Fermat's Little Theorem.

If p is prime and $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

- b. Compute $49^{323} \pmod{11}$

$$\text{So } 49^{323} \equiv 5^3 \pmod{11} \text{ as proved in class using Modular arith. \&}$$

$$\equiv 125 \equiv 4 \pmod{11} \text{ Fermat's Little Thm since 11 is prime.}$$

c. Prove that $7^{10k} - 12^k \pmod{11} = 0$ for any positive integer k

Fermat's Little Thm says $a^{10} \equiv 1 \pmod{11}$ if $11 \nmid a$. We have $a=7$.

Also $12 \equiv 1 \pmod{11}$, so $12^k \equiv 1^k \pmod{11}$, by rules of

Modular arithmetic. Using these congruences, we have

$$7^{10k} - 12^k \equiv (7^{10})^k - 1^k \equiv 1^k - 1^k \equiv 0 \pmod{11}.$$

Since $7^{10k} - 12^k \equiv 0 \pmod{11}$, this means that

$$7^{10k} - 12^k \pmod{11} = 0 \pmod{11} = 0.$$

4. INDUCTION

We have proved the rule of modular arithmetic that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$. Use this to prove by induction that if $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$ for all positive integers n . Point out the reasoning behind each step that you make.

The proof is by induction ^{on n} . $P(n)$ will be the statement that $a^n \equiv b^n \pmod{m}$. We are given that $a \equiv b \pmod{m}$.

Basis step: $P(1)$ says that $a^1 \equiv b^1 \pmod{m}$, which is true, because it was given.

Inductive step: We know $P(N)$, so that $a^N \equiv b^N \pmod{m}$ and we must show $P(N+1)$, so that $a^{N+1} \equiv b^{N+1} \pmod{m}$.

Using modular arithmetic and the given congruence $a \equiv b \pmod{m}$ together with the inductive hypothesis that $a^N \equiv b^N \pmod{m}$, we conclude that $a^{N+1} \equiv a^N \cdot a \equiv b^N \cdot b \equiv b^{N+1} \pmod{m}$ so $a^{N+1} \equiv b^{N+1} \pmod{m}$.

5. COMPLETE INDUCTION AND RECURSION

A sequence is defined by setting $a_1 = 2$, $a_2 = 4$, and $a_{n+1} = 3a_n - 2a_{n-1}$ for each integer $n \geq 2$.

Show that $a_n = 2^n$ for all positive integers n .

We prove $a_n = 2^n$ for all $n \in \mathbb{Z}^+$. The proof is by complete induction on n . $P(n)$ will be the statement $a_n = 2^n$.

Basis step: $P(1)$ says $a_1 = 2^1$. This is true because we are given $a_1 = 2$.

$P(2)$ says $a_2 = 2^2 = 4$. This is true because we are given $a_2 = 4$.

Inductive step. We must show $P(N+1)$ is true if we know $P(N), P(N-1), \dots$ are all true. $P(N)$ says $a_N = 2^N$ and $P(N-1)$ says $a_{N-1} = 2^{N-1}$.

We use these to find $a_{N+1} = 3a_N - 2a_{N-1}$, the definition of a_{N+1} . Substituting, we get $a_{N+1} = 3 \cdot 2^N - 2 \cdot 2^{N-1} = 3 \cdot 2^N - 2 \cdot 2^{N-1} = (3-1)2^N = 2 \cdot 2^N = 2^{N+1}$, so $a_{N+1} = 2^{N+1}$.

6. CHINESE REMAINDER THEOREM and EULER PHI FUNCTION

a. State the Chinese Remainder Theorem

Suppose that $\gcd(m, n) = 1$ and that $1 \leq a \leq m$ and $1 \leq b \leq n$. Then there is exactly one integer A in $\mathbb{Z}/mn\mathbb{Z}$ with $A \equiv a \pmod{m}$, and $A \equiv b \pmod{n}$.

- b. Make a table showing how the numbers from 1 to 21 fit into rows indicating their remainders mod 3 and columns indicating their remainders mod 7.

mod 7

	1	2	3	4	5	6	7	
<u>mod 3</u>	1	16	10	4	19	13	7	
	2	8	2	17	11	5	20	14
	3	15	9	3	18	12	6	21

- c. Use your table to find the unique integer between 1 and 21 which is congruent to 2 mod 3 and congruent to 3 mod 7.

17

- d. Evaluate $\phi(21)$, the value of the Euler phi function.

$$\begin{aligned}\phi(21) &= \phi(3 \cdot 7) = \phi(3) \phi(7) = (3-1)(7-1) \\ &= 2 \cdot 6 = 12\end{aligned}$$

- e. If a is an integer that is relatively prime to 21, show that $a^{\phi(21)} \equiv 1 \pmod{21}$, by showing that it is congruent to 1 modulo 7 and also congruent to 1 modulo 3.

$(a, 21) = 1 \Rightarrow 3 \nmid a$ so $a^{3-1} \equiv 1 \pmod{3}$ by Fermat's Little Theorem, since 3 is prime.
Also $(a, 21) = 1 \Rightarrow 7 \nmid a$ so $a^{7-1} \equiv 1 \pmod{7}$.

This means that we have $a^2 \equiv 1 \pmod{3}$

and $a^6 \equiv 1 \pmod{7}$.

So $a^{\phi(21)} = a^{12} = (a^2)^6 \equiv 1^6 \equiv 1 \pmod{3}$

and $a^{\phi(21)} = a^{12} = (a^6)^2 \equiv 1^2 \equiv 1 \pmod{7}$.

We see that $a^{\phi(21)} \equiv 1 \pmod{3}$ and

$a^{\phi(21)} \equiv 1 \pmod{7}$ and

Let $A = a^{\phi(21)} \pmod{21}$. We have $A \equiv 1 \pmod{3}$ and $A \equiv 1 \pmod{7}$. The Chinese Remainder Theorem tells us that the only possibility is $A = 1 = a^{\phi(21)} \pmod{21}$.