CS 70 Discrete Mathematics and Probability Theory
Spring 2017 Rao

DIS 3b

1 Modular Arithmetic

Solve the following equations for x and y modulo the indicated modulus, or show that no solution exists. Show your work.

(a) $9x \equiv 1 \pmod{11}$.

(b) $10x + 23 \equiv 3 \pmod{31}$.

(c) $3x + 15 \equiv 4 \pmod{21}$.

(d) The system of simultaneous equations $3x + 2y \equiv 0 \pmod{7}$ and $2x + y \equiv 4 \pmod{7}$.

Solution:

(a) $9x \equiv 1 \pmod{11}$: Multiply both sides by $9^{-1} \equiv 5 \pmod{11}$ to get $x \equiv 5 \pmod{11}$.

(b) $10x + 23 \equiv 3 \pmod{31}$: Subtract 23 from both sides, then multiply both sides by $10^{-1} = -3 \pmod{31}$ to find $x \equiv (-20) \cdot (-3) \equiv 60 \equiv 29 \pmod{31}$.

(c) $3x + 15 \equiv 4 \pmod{21}$: Subtract 15 from both sides to get $3x \equiv 10 \pmod{21}$. Now note that this implies $3x \equiv 1 \pmod{3}$, since 3 divides 21, and the latter equation has no solution, so the former cannot either.

(d) The *system* $3x + 2y \equiv 0 \pmod{7}, 2x + y \equiv 4 \pmod{7}$: First, subtract the first equation from double the second equation to get $2(2x + y) - (3x + 2y) \equiv x \equiv 1 \pmod{7}$; now plug in to the second equation to get $2 + y \equiv 4 \pmod{7}$, so the system has the solution $x \equiv 1 \pmod{7}$, $y \equiv 2 \pmod{7}$.

2 Baby Fermat

Assume that a does have a multiplicative inverse $\pmod{m}$. Let us prove that its multiplicative inverse can be written as $a^k \pmod{m}$ for some $k \geq 0$.

(a) Consider the sequence $a, a^2, a^3, \ldots \pmod{m}$. Prove that this sequence has repetitions.

(b) Assuming that $a^i \equiv a^j \pmod{m}$, where $i > j$, what can you say about $a^{i-j} \pmod{m}$?

(c) Prove that the multiplicative inverse can be written as $a^k \pmod{m}$. What is k in terms of i and j?

Solution:

(a) There are only m possible values $\pmod m$, and so after the m-th term we should see repetitions.

(b) We will temporarily use the notation a^* for the multiplicative inverse of a to avoid confusion. If we multiply both sides by $(a^*)^j$, we get

$$\begin{aligned} a^i &\equiv a^j && \pmod m, \\ a^{i-j}\underbrace{a\cdots a}_{j \text{ times}} &\equiv \underbrace{a\cdots a}_{j \text{ times}} && \pmod m, \\ a^{i-j}\underbrace{a\cdots a}_{j \text{ times}}\cdot\underbrace{a^*\cdots a^*}_{j \text{ times}} &\equiv \underbrace{a\cdots a}_{j \text{ times}}\cdot\underbrace{a^*\cdots a^*}_{j \text{ times}} && \pmod m, \\ a^{i-j} &\equiv 1 && \pmod m. \end{aligned}$$

(c) We can rewrite $a^{i-j} \equiv 1 \pmod m$ as $a^{i-j-1}a \equiv 1 \pmod m$. Therefore a^{i-j-1} is the multiplicative inverse of $a \pmod m$.

3 Does It Exist?

Can you find a number that is a perfect square and is a multiple of 2 but not a multiple of 4? Either give such a number or prove that no such number exists.

Solution:

No, such a number does not exist. In mathematical notation, we are asked to find a number x such that, for $n \in \mathbb{N}$, $4n+2 = x^2$ (since x cannot be $4n$, $4n+1$, or $4n+3$). Taking mod 4 of both sides, we get $x^2 \equiv 2 \pmod 4$. Does this number exist? We will determine this by cases.

We know that $x \pmod 4$ can have 4 different values:

- $x \mod 4 = 0$. Then $x^2 \equiv 0 \pmod 4$.
- $x \mod 4 = 1$. Then $x^2 \equiv 1 \pmod 4$.
- $x \mod 4 = 2$. Then $x^2 \equiv 4 \equiv 0 \pmod 4$.
- $x \mod 4 = 3$. Then $x^2 \equiv 9 \equiv 1 \pmod 4$.

Therefore we can see it is impossible to find such a number; no matter what x is, x^2 will never be a multiple of 4 plus 2.

4 Bijections

Let n be an odd number. Let $f(x)$ be a function from $\{0,1,\ldots,n-1\}$ to $\{0,1,\ldots,n-1\}$. In each of these cases say whether or not $f(x)$ is necessarily a bijection. Justify your answer (either prove $f(x)$ is a bijection or give a counterexample).

(a) $f(x) = 2x \pmod{n}$.

(b) $f(x) = 5x \pmod{n}$.

(c) n is prime and

$$f(x) = \begin{cases} 0 & \text{if } x = 0, \\ x^{-1} \pmod{n} & \text{if } x \neq 0. \end{cases}$$

(d) n is prime and $f(x) = x^2 \pmod{n}$.

Solution:

(a) Bijection, because there exists the inverse function $g(y) = 2^{-1}y \pmod{n}$. Since n is odd, $\gcd(2,n) = 1$, so the multiplicative inverse of 2 exists.

(b) Not necessarily a bijection. For example, $n = 5, f(0) = f(1) = 0$.

(c) Bijection, because the multiplicative inverse is unique.

(d) Definitely not a bijection. For example, if $n = 3$, $f(1) = f(2) = 1$.