SAMPLE MATH 55 MIDTERM 1, SPRING 2014

(1) Mark each of the following questions true (T) or false (F). Provide a sentence or two justifying each answer.

(a) If $x \equiv y \pmod{m}$ then $ax \equiv ay \pmod{m}$. T.

If $m \mid (x-y)$ then $m \mid a(x-y)$.

(b) If $ax \equiv ay \pmod{m}$ then $x \equiv y \pmod{m}$. F.

$2 \cdot 4 \equiv 2 \cdot 2 \mod 4$ but $4 \not\equiv 2 \mod 4$.

(c) The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = \lfloor \frac{x}{2} \rfloor$ is surjective. T.

Given any $y \in$ codomain ($\mathbb{Z}$),
$f(2y) = y$.

(d) $f(S \cap T) = f(S) \cap f(T)$. F.

Counterexample: $f : X \longrightarrow Y$

$x_1 \bullet \longrightarrow \bullet\, y$
$x_2 \bullet \longrightarrow$

Let $S = \{x_1\}$
$T = \{x_2\}$.

$f(S \cap T) = \emptyset$ but
$f(S) \cap f(T) = \{y\}$.

(e) The positive real numbers are countable. F.

Reals are uncountable.

(f) Let $\mathbb{R}$ be the domain, and let $P(x, y)$ be the statement $y^2 = x$. Determine the truth value of the following statement:
$\forall x \exists y\, P(x, y)$. F.

If $x = -1$, $\nexists\, y \in \mathbb{R}$
s.t. $y^2 = -1$.

(2) Prove that if m is a positive integer of the form $4k+3$ for some non-negative integer k, then m is not the sum of the squares of two integers.

Contradiction. Assume $m = a^2+b^2$ for $a,b \in \mathbb{Z}$.

Lemma: For $a \in \mathbb{Z}$, $a^2 \bmod 4$ is 0 or 1.

Pf: If a is even, $a = 2k$ for $k \in \mathbb{Z}$,
So $a^2 \bmod 4$ is $4k^2 \bmod 4 = 0$.
If a is odd, $a = 2k+1$ for $k \in \mathbb{Z}$,
So $a^2 \bmod 4 = (2k+1)^2 \bmod 4 = 4k^2+4k+1 = 1 \bmod 4$.

Now using the lemma,
Since $m = a^2+b^2$,
$m \bmod 4$ is either:
$$0^2+0^2 = 0$$
$$1^2+1^2 = 2$$
$$0^2+1^2 = 1$$

$\therefore$ $m \bmod 4$ is $0, 1,$ or 2.

But if $m = 4k+3$, $m \bmod 4 = 3$. $\Rightarrow\Leftarrow$

(3) Prove that $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

We need to show that

$x \in \overline{A \cup B}$ iff $x \in \overline{A} \cap \overline{B}$.

$x \in \overline{A \cup B} \iff$

$x \notin A \cup B \iff$

$x \notin A$ and $x \notin B \iff$

$x \in \overline{A}$ and $x \in \overline{B} \iff$

$x \in \overline{A} \cap \overline{B}$.

$\boxed{\checkmark}$

(4) Computation.

- Write the number 466 in base 9.

$466 = 51\cdot 9 + 7$

$51 = 5\cdot 9 + 6$

$5 = 0\cdot 9 + 5$

7

67

567

$\boxed{\therefore\ 466 = (567)_9.}$

Check: $466 = 5\cdot 9^2 + 6\cdot 9 + 7$ ✓

- Does an inverse of 8 (mod 75) exist? If so, find one. yes — $\gcd(8,75)=1$.

$75 = 9\cdot 8 + 3 \Rightarrow$ ① $3 = 75 - 9\cdot 8$

$8 = 2\cdot 3 + 2 \Rightarrow$ ② $2 = 8 - 2\cdot 3$

$3 = 1\cdot 2 + 1 \Rightarrow$ ③ $1 = 3 - 1\cdot 2$

$2 = 2\cdot 1 + 0$

By ③, $1 = 3 - 1\cdot 2 \overset{\text{by ②}}{=} 3 - 1\cdot(8 - 2\cdot 3) = 3\cdot 3 - 1\cdot 8$

$\overset{\text{by ①}}{=} 3\cdot(75 - 9\cdot 8) - 1\cdot 8 = 3\cdot 75 - 28\cdot 8$

So $3\cdot 75 - 28\cdot 8 = 1 \Rightarrow -28\cdot 8 \equiv 1 \mod 75$.

So -28 is an inverse of 8 mod 75.

Also since $-28 \equiv 47 \mod 75$, $\boxed{47 \text{ is an inverse of } 8 \bmod 75.}$

- Calculate $6^{666} \bmod 23$.

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

$\therefore\ 6^{22} \equiv 1 \mod 23$

$6^{666} = (6^{22})^{30}\cdot 6^6 = \underbrace{6^{22\cdot 30}}_{\equiv 1}\cdot 6^6 \equiv 1\cdot 6^6 \mod 23.$

↖ simplify

Now $6^6 = 36^3 \equiv 13^3 \mod 23$

$13^3 \equiv (-10)^3 \equiv -1000 \mod 23 = 12$ (Since $-1000 = 23(-44) + 12$)

So $6^{666} \equiv 12 \mod 23 = 12$.

(5) Prove that if p is prime, the only solutions of $x^2 \equiv 1 \pmod{p}$ are integers x such that $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.

Suppose that $x^2 \equiv 1 \pmod{p}$.

Then $p \mid (x^2 - 1) \implies$

$p \mid (x-1)(x+1)$.

Since p is prime, $p \mid (x-1)$ or $p \mid (x+1)$.

So $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.

$\blacksquare$

(6) Find all solutions to the system of congruences $x \equiv 2 \pmod 3$, $x \equiv 1 \pmod 4$, and $x \equiv 3 \pmod 5$.

Let $m_1 = 3$, $m_2 = 4$, $m_3 = 5$. Let $a_1 = 2$, $a_2 = 1$, $a_3 = 3$.

There is a unique solution mod $m = 3 \cdot 4 \cdot 5 = 60$.

Let $M_1 = \frac{m}{m_1} = 20$.

Let $M_2 = \frac{m}{m_2} = 15$.

Let $M_3 = \frac{m}{m_3} = 12$.

Since $\gcd(m_1, M_1) = \gcd(3, 20) = 1$,
$\exists\, y_1$ s.t. $20 y_1 \equiv 1 \bmod 3$. Can use $y_1 = 2$.

Since $\gcd(m_2, M_2) = \gcd(4, 15) = 1$,
$\exists\, y_2$ s.t. $15 y_2 \equiv 1 \bmod 4$. Can use $y_2 = 3$.

Since $\gcd(m_3, M_3) = \gcd(5, 12) = 1$,
$\exists\, y_3$ s.t. $12 y_3 \equiv 1 \bmod 5$. Can use $y_3 = 3$.

Now let
$$\begin{aligned} x &= a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \\ &= 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 \\ &= 80 + 45 + 108 \\ &\equiv 20 + 45 + 48 \mod 60 \\ &\equiv 53 \mod 60. \end{aligned}$$

$\therefore$ the solutions to the system are all integers congruent to 53 mod 60, ie.

$\{ 53 + 60\ell \mid \ell \in \mathbb{Z} \}$.