

MATH 115, SUMMER 2012
MOCK QUIZ, LECTURE 9

JAMES MCIVOR

Pretend this is a real quiz and take. It's not for a grade, though. First look for the ones you already know how to do. We'll go over it at the end, but use it as a guide to see what you should study most for tomorrow's (real) quiz.

(1) (CRT problem)

Solve the system of congruences, if possible. If not possible, explain why not.

$$x \equiv 13 \pmod{20}$$

$$x \equiv 3 \pmod{15}$$

$$x \equiv 9 \pmod{12}$$

(2) (Solving one linear congruence)

Find all integers x satisfying the congruence

$$12x \equiv 16 \pmod{20}$$

Then give an integer b for which the congruence $12x \equiv b \pmod{20}$ has no solution, and say briefly why not.

(3) (Algebra Questions)

(a) Give an example of a ring, and an element of this ring which is neither a unit nor a zerodivisor.

(b) Explain why there are no ring homomorphisms from $\mathbb{Z}/2$ to \mathbb{Z}/m , for any $m > 2$.

(c) Compute $(2, 4) + (1, 3)$ and $(2, 4) \cdot (1, 3)$ in the ring $\mathbb{Z}/3 \times \mathbb{Z}/5$.

(d) The Chinese Remainder Theorem says that there is an isomorphism ϕ from $\mathbb{Z}/3 \times \mathbb{Z}/5$ to $\mathbb{Z}/15$. What is $\phi(2, 3)$?

(4) Suppose $p > 2$ is a prime that divides $26^2 + 64^2 = 4672$. What is the remainder when p is divided by 4?

- ① First, split moduli into prime powers since they're not relatively prime.

$$\begin{aligned} x \equiv 13 \pmod{20} &\rightarrow x \equiv 13 \equiv 1 \pmod{4} \\ &x \equiv 13 \equiv 3 \pmod{5} \end{aligned}$$

$$\begin{aligned} x \equiv 3 \pmod{15} &\rightsquigarrow x \equiv 3 \equiv 0 \pmod{3} \\ &x \equiv 3 \pmod{5} \end{aligned}$$

$$\begin{aligned} x \equiv 9 \pmod{12} &\rightsquigarrow x \equiv 9 \equiv 0 \pmod{3} \\ &x \equiv 9 \equiv 1 \pmod{4} \end{aligned}$$

These congruences are consistent.
The new system is

$$\begin{aligned} x &\equiv 0 \pmod{3} \\ x &\equiv 1 \pmod{4} \\ x &\equiv 3 \pmod{5} \end{aligned}$$

To solve this, set $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $M = m_1 m_2 m_3 = 60$

$$\begin{aligned} \text{Find inverse of } \frac{m}{m_1} \pmod{m_1} &: 20^{-1} \pmod{3} \equiv 2^{-1} \pmod{3} = \boxed{2} = b_1 \\ \text{Find inverse of } \frac{m}{m_2} \pmod{m_2} &: 15^{-1} \pmod{4} \equiv 3^{-1} \pmod{4} = \boxed{3} = b_2 \\ \text{Find inverse of } \frac{m}{m_3} \pmod{m_3} &: 12^{-1} \pmod{5} \equiv 2^{-1} \pmod{5} = \boxed{3} = b_3 \end{aligned}$$

$$\begin{aligned} \text{Set } x = 20 \cdot 2 \cdot 0 + 15 \cdot 3 \cdot 1 + 12 \cdot 3 \cdot 3 &\equiv 45 + 108 = 153 \equiv 33 \pmod{60} \end{aligned}$$

$$\boxed{x \equiv 33 \pmod{60}}$$

- ② $\gcd(17, 20) = 1 \mid 16$, so there is a solution. To find it,

$$\text{divide through by } g: 3x \equiv 4 \pmod{5}, \quad 3^{-1} \pmod{5} \rightarrow 2,$$

$$\begin{aligned} \therefore 2 \cdot 3x &\equiv 2 \cdot 4 \pmod{5} \\ \Rightarrow x &\equiv 8 \equiv 3 \pmod{5} \end{aligned}$$

$$\boxed{x \equiv 3 \pmod{5}}$$

If $4 \nmid b$, there is no solution, eg $12x \equiv 1 \pmod{20}$.

- ③ (a) \mathbb{Z} is a ring, in which 2 is neither a unit nor a zero divisor.
 $\mathbb{C}[x]$ is a ring, in which $3+x^2$ is neither a unit nor zero divisor.

(b) Suppose $f: \mathbb{Z}/2 \rightarrow \mathbb{Z}/m$ is a ring map, w/ $m > 2$.

$$\text{Then } 0 = 1+1 \text{ in } \mathbb{Z}/2 \Rightarrow$$

$$f(0) = f(1) + f(1) \text{ in } \mathbb{Z}/m$$

$$\Rightarrow 0 = 1+1 \text{ in } \mathbb{Z}/m, \text{ but } 2 \neq 0 \text{ in } \mathbb{Z}/m$$

for $m > 2$, contradiction.

$$(c) \text{ In } \mathbb{Z}/3 \times \mathbb{Z}/5, (2,4) + (1,3) = (2+1, 4+3) = (3,7) = \boxed{(0,2)}$$

$$(2,4) \cdot (1,3) = (2 \cdot 1, 4 \cdot 3) = (2,12) = \boxed{(2,2)}$$

(d) Let $\phi(2,3) = x \in \mathbb{Z}/15$.

$$\text{Then } x \equiv 2 \pmod{3} \Rightarrow x = 2 \text{ or } 5 \text{ or } 8 \text{ or } 11 \text{ or } 14$$

$$\text{and } x \equiv 3 \pmod{5} \Rightarrow x = 3 \text{ or } 8 \text{ or } 13$$

$$\text{So } \boxed{x=8}$$

④ Use: If $q \equiv 3 \pmod{4}$ and $q | a^2 + b^2$, then $q | a$ and $q | b$.

Since $p > 2$, $p \equiv 1 \pmod{4}$ or $p \equiv 3 \pmod{4}$.

If $p \equiv 3 \pmod{4}$, then $p | 26$ and $p | 64 \Rightarrow p = 2$

But $p > 2$, contradiction. So $p \equiv 1 \pmod{4}$, i.e.,

$\frac{p}{4}$ gives remainder 1.