

Solution

MATH 115, SUMMER 2012 QUIZ 2

JAMES MCIVOR

There are problems on the back of this page. Write clearly and in complete sentences. If you need extra paper, ask me.

- (1) (6 points) Solve the system of congruences, if possible. If not possible, explain why not.

$$x = a_1 \frac{m}{m_1} b_1 + a_2 \frac{m}{m_2} b_2 \\ + a_3 \frac{m}{m_3} b_3 \\ = 1 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot (-1) \\ + 3 \cdot 12 \cdot 3 \\ = 40 - 45 + 108 = 103$$

$$\begin{aligned} x &\equiv 7 \pmod{12} \\ x &\equiv 3 \pmod{20} \\ x &\equiv 7 \pmod{12} \Leftrightarrow \begin{cases} x \equiv 7 \equiv 3 \pmod{4} \\ x \equiv 7 \equiv 1 \pmod{3} \end{cases} \text{ consistent!} \\ x &\equiv 3 \pmod{20} \Leftrightarrow \begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 3 \pmod{5} \end{cases} \\ m &= 3 \cdot 4 \cdot 5 = 60 \\ b_1 &= \left(\frac{m}{m_1}\right)^{-1} = 20^{-1} \pmod{3} = 2 \\ b_2 &= \left(\frac{m}{m_2}\right)^{-1} = 15^{-1} \pmod{4} = -1 \\ b_3 &= \left(\frac{m}{m_3}\right)^{-1} = 12^{-1} \pmod{5} = 3 \end{aligned}$$

- (2) (3 points) Explain why 101 divides $(100! + 1)$ [Hint: 101 is prime]

By Wilson's Thm, $100! \equiv -1 \pmod{101}$

which means $101 \mid 100! + 1$

- (3) (3 points) For which integers $m > 1$ does the ring \mathbb{Z}/m have no zero divisors?

m prime.

If m is composite, say $m = p_1^{a_1} \cdots p_r^{a_r}$,

by CRT, $\mathbb{Z}/m \cong \mathbb{Z}/p_1^{a_1} \times \cdots \times \mathbb{Z}/p_r^{a_r}$,

and product rings always have zero divisors

$$(1, 0, \dots, 0) \cdot (0, 1, 0, \dots, 0) = (0, 0, 0, \dots, 0)$$

- (4) (3 points) The Chinese Remainder Theorem says that there is an isomorphism ψ from $\mathbb{Z}/4 \times \mathbb{Z}/5$ to $\mathbb{Z}/20$. What is $\psi(1, 3)$?

If $\psi(1, 3) = x \in \mathbb{Z}/20$, then $x \equiv 1 \pmod{4}$
and $x \equiv 3 \pmod{5}$

$x \equiv 1 \pmod{4} \Rightarrow x = 1 \text{ or } 5 \text{ or } 9 \text{ or } 13 \text{ or } 17$

The only one congruent to 3 mod 5 is

$$\boxed{x = 13}$$

- (5) (1 point each) True or False. No justification necessary.

- (a) There are integers a, b such that $980 = a^2 + b^2$.

True:

$$980 = 2 \cdot 490 = 2^2 \cdot 5 \cdot 7^2$$

7 is only prime $\equiv 3 \pmod{4}$
in factorization, and
its exponent is even.

- (b) If $f: R \rightarrow S$ is a ring homomorphism and $r \in R$ is a unit, then $f(r)$ is a unit in S .

True:

If r is a unit, $\exists r' \text{ w/ } rr' = 1$, so

$$f(rr') = f(1)$$

- (c) $6^{145} \equiv 1 \pmod{13}$.

False

By Fermat's Little Thm,

$$6^{12} \equiv 1$$

$\Rightarrow 6^{145} \equiv 6 \pmod{13}$

$$\Rightarrow f(r) f(r') = 1$$

$\Rightarrow f(r)$ a unit

- (d) The congruence

$$8x \equiv 7 \pmod{22}$$

has solutions.

False

gcd of 8 and 22 is 2, but $2 \nmid 7$

- (e) If $m > 1$ is odd, then $\phi(m) = \phi(2m)$ (here ϕ is Euler's totient function).

True

If m is odd, $(2, m) = 1$

$$\begin{aligned} \phi(2m) &= \phi(2)\phi(m) = 1 \cdot \phi(m) \\ &= \phi(m) \end{aligned}$$