

## Homework 5 Due Wednesday, Oct 1

**Problem 1.** A band of 13 pirates stole a sack of coins. When they tried to divide them equally among them, 2 coins remained. In the brawl that followed, two pirates were killed. Again, they tried to divide the coins equally, only to find 7 coins remaining. Four more pirates were killed! Now, when they tried to divide the coins 3 were left. The pirates became very upset and frustrated and they shot each other. You came across their sack of coins. What is the smallest amount of coins you own now?

**Problem 2.** Consider a system of congruences

$$\begin{aligned}x &\equiv a \pmod{m} \\x &\equiv b \pmod{n}\end{aligned}$$

Let  $d = \gcd(m, n)$

- (a) Show that if this system has a solution then  $d \mid a - b$ .
- (b) Show that if  $d \mid a - b$  then the system has a solution. Hint: Since  $d = \gcd(m, n)$  there exist  $s$  and  $t$  such that  $d = ms + nt$ . Let

$$x = b + nt \frac{a - b}{d}.$$

Show that  $x$  is a solution of the system.

**Problem 3.** A commutative ring with unity is called a *field* if every nonzero element is a unit. For which values of  $m$  is  $\mathbb{Z}_m$  a field? (Use our description of units in  $\mathbb{Z}_m$ :  $a \in \mathbb{Z}_m$  is a unit if and only if  $\gcd(a, m) = 1$ ).

**Problem 4.**

- (a) Show that if  $p$  is prime and  $a^2 \equiv 1 \pmod{p}$ , then  $a \equiv 1 \pmod{p}$  or  $a \equiv -1 \pmod{p}$ . Note that this says that the only two units in  $\mathbb{Z}_p$  that are equal to their multiplicative inverses are 1 and  $p - 1$  (same as  $-1$  modulo  $p$ ).
- (b) **Wilson's Theorem:** Let  $p$  be prime show that

$$(p - 1)! \equiv -1 \pmod{p}.$$

Hint: Check the theorem for  $p = 2$  and  $p = 3$  directly. Let  $p > 3$  and note that  $p - 3$  is even. Look at the elements of  $\mathbb{Z}_p = \{1, 2, \dots, p - 2, p - 1, p\}$ . What happens if we multiply them all modulo  $p$ ? Which ones will cancel? Use part (a).

**Problem 5.** In  $\mathbb{Z}$  we have the following property: If  $ab = 0$  then either  $a = 0$  or  $b = 0$ . Rings that satisfy this property are called *integral domains*. Is  $\mathbb{Z}_{12}$  an integral domain? What about  $\mathbb{Z}_p$  where  $p$  is prime? (Hint: use the fact that every nonzero element in  $\mathbb{Z}_p$  is a unit.) What about  $\mathbb{Z}_m$  where  $m$  is composite?

**Problem 6.** Let  $M_{2,2}(\mathbb{R})$  be the ring of 2 by 2 matrices with real entries. Describe the units of  $M_{2,2}(\mathbb{R})$ .