

Ch. 3: 7, 8, 9, 16.

7.) a) Let  $p$  be prime. Suppose  $a$  &  $b$  are integers such that  $ab \equiv 0 \pmod{p}$ . Show either  $a \equiv 0$  or  $b \equiv 0 \pmod{p}$ .

if  $ab \equiv 0 \pmod{p}$  then  $p \mid ab$   
2 cases

if  $a \equiv 0 \pmod{p}$  then  $p \mid a \rightarrow p \mid ab$   
if  $b \equiv 0 \pmod{p}$  then  $p \mid b \rightarrow p \mid ab$

b) Show that if  $a, b, n$  are integers with  $n \mid ab$  and  $\gcd(a, n) = 1$ , then  $n \mid b$ .

if  $n \mid ab$  then  $ab \equiv 0 \pmod{n}$   
and if  $\gcd(a, n) = 1$  then  $a$  &  $n$  are relatively prime meaning  $n \nmid a$ . Therefore if  $n \mid ab$  and  $n \nmid a$  then  $n \mid b$ .

8.) Let  $p \geq 3$  be prime. Show that the only solutions to  $x^2 \equiv 1 \pmod{p}$  are  $x \equiv \pm 1 \pmod{p}$ .

$$x^2 \equiv 1 \pmod{p} \rightarrow x^2 - 1 \equiv 0 \pmod{p}$$

factor

$(x+1)(x-1) \equiv 0 \pmod{p}$   
from (7a.) we know that if  $a = x+1$  and  $b = x-1$  that since their product is congruent to  $0 \pmod{p}$  that either  $p \mid a$  or  $p \mid b$

9.) Suppose  $x \equiv 2 \pmod{7}$  and  $x \equiv 3 \pmod{10}$   
 what is congruent to  $\pmod{70}$ ?

First we find the multiplicative inverse of 1

Chinese  
Remainder  
Theorem

$$\begin{aligned}
 &7 \pmod{10} & 10 &= 7 \cdot 1 + 3 \\
 &7a + 10b = 1 & 7 &= 3 \cdot 2 + 1 \\
 &a = 3 \quad b = -2 & 1 &= 7 - 3 \cdot 2 \\
 &7^{-1} = 3 \pmod{10} & 1 &= 7 - 2(10 - 7) \\
 & & 1 &= 7 - 3 - 2 \cdot 10
 \end{aligned}$$

$$\begin{aligned}
 K &= (3 - 2)3 \equiv 3 \pmod{10} \\
 x &\equiv (2 + 7)3 \equiv 27 \pmod{70}
 \end{aligned}$$

16.) a) let  $p = 7, 13$  or  $19$ . Show that  $a^{1728} \equiv 1 \pmod{p}$   
 for all  $a$  with  $\gcd(a, p) = 1$ .

if  $\gcd(a, p) = 1$

$$1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024$$

$$1728 = 1024 + 512 + 128 + 64$$

$$\Rightarrow a^{1024} \cdot a^{512} \cdot a^{128} \cdot a^{64}$$

by Fermat's little theorem we know

$$\begin{aligned}
 a^6 &\equiv 1 \pmod{7} \\
 a^{12} &\equiv 1 \pmod{13} \\
 a^{18} &\equiv 1 \pmod{19}
 \end{aligned}$$

Since 1728 is divisible by 6, 12, and 18  
 we know that  $a^{1728}$  can be made of  
 a linear combination  $\equiv 1 \pmod{7}, 1 \pmod{13}, 1 \pmod{19}$ .

b.) Let  $p = 7, 13, \text{ or } 19$ . Show that  $a^{1729} \equiv a \pmod{p}$  for all  $a$ .

From (a) we know  $a^{1728} \equiv 1 \pmod{p}$  for  $p = 7, 13, \text{ or } 19$ . We can simply multiply this by  $a$  to get:

$$\begin{aligned} a^{1728} \cdot a &\equiv 1 \cdot a \pmod{p} \\ \rightarrow a^{1729} &\equiv a \pmod{p} \checkmark \end{aligned}$$

Q Show that  $a^{1729} \equiv a \pmod{1729}$  for all  $a$

$$1729 = 7 \cdot 13 \cdot 19.$$

Chinese remainder theorem

$$x \equiv a \pmod{7}$$

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

$$x \equiv a \pmod{19}$$

