

Math 111, HW 5

Curtis Paul

May 13, 2007

16. Using the Euclidean algorithm, we get

$$1 = 13(7) - 2(45),$$

$$1 = 2(63) - 25(5), \text{ and}$$

$$1 = 4(9) - 35.$$

So, $-90 \equiv 1 \pmod{7}$, $126 \equiv 1 \pmod{5}$, and $-35 \equiv 1 \pmod{9}$. This gives us $x = -90 + 4(-35) + 3(126) = 148$.

19.

$$x^2 - 1 \equiv 0 \pmod{p^a}, \text{ so}$$

$$(x+1)(x-1) \equiv 0 \pmod{p^a}.$$

Let $x+1 = p^i m$, $x-1 = p^j n$, where $p \nmid m$, $p \nmid n$. Note that $i+j \geq a$.

$$\text{If } i < j, 2 = (x+1) - (x-1) = p^i m - p^j n = p^i(m - p^{j-i}n),$$

so $i = 0$, $j \geq a$, and therefore $x-1 \equiv 0 \pmod{p^a}$, yielding $x \equiv 1 \pmod{p^a}$.

$$\text{If } i > j, 2 = (x+1) - (x-1) = p^i m - p^j n = p^j(p^{i-j}m - n),$$

so $j = 0$, $i \geq a$, and therefore $x+1 \equiv 0 \pmod{p^a}$, yielding $x \equiv -1 \pmod{p^a}$.

$$\text{If } i = j, 2 = (x+1) - (x-1) = p^i m - p^j n = p^j(m - n),$$

so $i = j = 0$. This violates $i+j \geq a$, so this case doesn't occur.

20. If $b = 1, 2$, just check. If $b \geq 3$,

$$x^2 - 1 \equiv 0 \pmod{2^b}, \text{ so}$$

$$(x+1)(x-1) \equiv 0 \pmod{2^b}.$$

Let $x+1 = 2^i m$, $x-1 = 2^j n$, where $2 \nmid m$, $2 \nmid n$. Note that $i+j \geq b$.

$$\text{If } i < j, 2 = (x+1) - (x-1) = 2^i m - 2^j n = 2^i(m - 2^{j-i}n),$$

so $i = 1$, $j \geq b-1$, and therefore $x-1 \equiv 0$ or $2^{-1} \pmod{2^b}$, yielding $x \equiv 1$ or $2^{-1} + 1 \pmod{2^b}$.

$$\text{If } i > j, 2 = (x+1) - (x-1) = 2^i m - 2^j n = 2^j(p^{i-j}m - n),$$

so $j = 1$, $i \geq b-1$, and therefore $x+1 \equiv 0$ or $2^{-1} \pmod{2^b}$, yielding $x \equiv -1$ or $2^{-1} + 1 \pmod{2^b}$.

$$\text{If } i = j, 2 = (x+1) - (x-1) = 2^i m - 2^j n = 2^j(m - n),$$

with $m-n$ even, so $i = j = 0$, which cannot happen.