

Math 104A, Practice Midterm 2, Fall 2002.

1(a). Solve $x^2 + 5 \equiv 0 \pmod{49}$.

Modulo 7 we have

$x \pmod{7}$	0	1	2	3	4	5	6
$x^2 \pmod{7}$	0	1	4	2	2	4	1

The solutions to $x^2 + 5 \equiv 0 \pmod{7}$ or $x^2 \equiv 2 \pmod{7}$ are $x = 3$ and $x = 4$.

Now writing $f(x) = x^2 + 5$ we have

x	3	4
f	14	21
f'	6	8

Since $f'(x_0) \neq 0$, for $x_0 = 3, 4$, we a solution to $f \equiv 0 \pmod{49}$ corresponding to each of $x_0 = 3$ and $x_0 = 4$. They have the form $x = x_0 + 7t$ where t solves $f(x_0) + 7tf'(x_0) \equiv 0 \pmod{49}$. We solve this. The first solution is $x = 3 + 7t$ where

$$\begin{aligned} 14 + 7 \cdot 6t &\equiv 0 \pmod{49} \Rightarrow 2 + 6t \equiv 0 \pmod{7} \Rightarrow 6t \equiv -2 \pmod{7} \Rightarrow -t \equiv -2 \pmod{7} \\ &\Rightarrow t \equiv 2 \pmod{7} \Rightarrow x \equiv 3 + 2 \cdot 7 \equiv 17 \pmod{49}. \end{aligned}$$

The second solution is $x = 4 + 7t$ where

$$\begin{aligned} 21 + 7 \cdot 8t &\equiv 0 \pmod{49} \Rightarrow 3 + 8t \equiv 0 \pmod{7} \Rightarrow 8t \equiv 4 \pmod{7} \Rightarrow t \equiv 4 \pmod{7} \\ &\Rightarrow x \equiv 4 + 4 \cdot 7 \equiv 32 \pmod{49}. \end{aligned}$$

(b). Solve $x^2 + 5 \equiv 0 \pmod{35}$.

Modulo 5 we have that the only solution is $0 \pmod{5}$, so x satisfies

$$\begin{cases} x \equiv 0 \pmod{5} \\ x \equiv 3 \text{ or } 4 \pmod{7} \end{cases}$$

To solve this Chinese remainder problem you can use the formula or solve as follows

$$\begin{cases} x \equiv 0 \pmod{5} \\ x \equiv a \pmod{7} \end{cases}$$

$x = 5k \equiv a \pmod{7}$ hence $k \equiv 3a \pmod{7}$ hence $k = 3a + 7j$ and $x = 15a + 35j$. Plugging in $a = 3$ or 4 gives $x = 10$ or $25 \pmod{35}$.

2. (a). Show that if $(m, a) | b$ then the congruence

$$ax \equiv b \pmod{m}$$

has a solution. You may assume any result proved in Chapter 2 of the book, but you must justify any statement concerning congruences.

Since $(m, a) = 1$, we can find u and v with $(m, u) = mu + av$. But since $(m, u) | b$ we can find c with $(m, u)c = b$. Then

$$b = (m, u)c = muc + avc,$$

and so setting $x = vc$ we have $b \equiv ax \pmod{m}$.

(b). Find all solutions x modulo 21 to the equation

$$6x \equiv 15 \pmod{21}.$$

Note that $(6, 21) = 3 | 15$. Now dividing the equation by 3, it is equivalent to

$$2x \equiv 5 \pmod{7}.$$

If this is satisfied then

$$x \equiv 4 \cdot 2x \equiv 4 \cdot 5 \equiv 20 \equiv 6 \pmod{7}.$$

This is the unique solution. It corresponds to $x \equiv 6, 13, 20 \pmod{21}$.

3. Show that there are infinitely many primes of the form $4k + 1$.

Suppose that p_1, \dots, p_r is a list of primes of the form $4k + 1$ and consider

$$(*) \quad N = (2p_1 \cdots p_r)^2 + 1.$$

Let p be a prime divisor of N . Then p is not in the set of primes $\{2, p_1, \dots, p_r\}$ since clearly these are all relatively prime to N . Now from the definition (*)

$$(*) \quad (2p_1 \cdots p_r)^2 \equiv -1 \pmod{p}$$

Hence $(2p_1 \cdots p_r)^4 \equiv 1 \pmod{p}$. Since $(2p_1 \cdots p_r)^4 \equiv 1 \pmod{p-1}$ and $(p-1, 4)$ can be written as $(p-1)u + 4v$, we have $(2p_1 \cdots p_r)^{(p-1, 4)} \equiv 1 \pmod{p}$. Now $(p-1, 4)$ cannot be 1 or 2 since this would contradict (*). (Here we use that $p \neq 2$.) Hence $(p-1, 4) = 4$ and so $4 | p-1$ and $p = 4k + 1$ for some k .

We just showed that if we have a finite list of primes of the form $4k + 1$ then we can always find a new one not in this list, and hence there are infinitely many primes of this form.

4. (a). State Euler's Theorem.

If $(x, m) = 1$ then $x^{\phi(m)} \equiv 1 \pmod{m}$.

(b). Find the smallest positive number ℓ such that for every integer x with $(x, 40) = 1$, we have $x^\ell \equiv 1 \pmod{40}$, and explain your answer.

Now $40 = 2^3 \cdot 5$ and $\phi(8) = 4$ and $\phi(5) = 4$. Now if $(x, 40) = 1$ then $(x, 8) = 1$ and $(x, 5) = 1$. Hence

$$x^4 \equiv 1 \pmod{8}, \qquad x^4 \equiv 1 \pmod{5}.$$

By the Chinese remainder theorem $x^4 \equiv 1 \pmod{40}$ (You can easily see this without CRT in fact). To see that 4 is the smallest exponent which will work, note that $3^2 = 9 \not\equiv 1 \pmod{40}$ and $3^3 = 27 \not\equiv 1 \pmod{40}$.