HW4 Joseph Schmidt

1. $y \equiv 1 \pmod 2$
$y \equiv 1 \pmod 7$ $\Rightarrow$
$y \equiv 1 \pmod{11}$
$y \equiv 0 \pmod{13}$

$M = m_1 \cdot m_2 \cdot m_3 \cdot m_4$
$= 2 \cdot 7 \cdot 11 \cdot 13 = 2002$

$M_1 = \frac{2002}{2} = 1001$
$M_2 = \frac{2002}{7} = 286$
$M_3 = \frac{2002}{11} = 182$
$M_4 = \frac{2002}{13} = 154$

$1001 y_1 \equiv 1 \pmod 2 \Rightarrow 1000y_1 + y_1 \equiv 1 \pmod 2$
$286 y_2 \equiv 1 \pmod 7$ $\quad 280y_2 + 6y_2 \equiv 1 \pmod 7$
$182 y_3 \equiv 1 \pmod{11}$ $\quad 176y_3 + 6y_3 \equiv 1 \pmod{11}$
$154 y_4 \equiv 1 \pmod{13}$ $\quad 143y_4 + 11y_4 \equiv 1 \pmod{13}$

$y_1 \equiv 1 \pmod 2 \Rightarrow y_1 \equiv 1 \pmod 2$
$\overline{6}\, 6 y_2 \equiv \overline{6}\, 1 \pmod 7$ $\quad y_2 \equiv 6 \pmod 7$
$\overline{6}\, 6 y_3 \equiv \overline{6}\, 1 \pmod{11}$ $\quad y_3 \equiv 2 \pmod{11}$
$\overline{11}\, 11 y_4 \equiv \overline{11}\, 1 \pmod{13}$ $\quad y_4 \equiv 6 \pmod{13}$

$y_1 = 1 \quad y_2 = 6 \quad y_3 = 2 \quad y_4 = 6$

$x_0 = 1 \cdot 1001 \cdot 1 + 6 \cdot 286 \cdot 1 + 2 \cdot 182 \cdot 1 + 6 \cdot 154 \cdot 0$
$x_0 = 3081$

$3081 \equiv 1079 \pmod{2002}$

2. $2x + 3y \equiv 5 \pmod 7$ — ①

$x + 5y \equiv 6 \pmod 7$ — ②

$\Downarrow$

$2x + 3y \equiv 5 \pmod 7$ — ①

$2x + 10y \equiv 12 \pmod 7$ — ② $\times 2$

$\Downarrow$

$-7y \equiv -7 \pmod 7$ — ① − ②

$y = 0$

$2x + 3(0) \equiv 5 \pmod 7$ — sub y into ②

$2x \equiv 5 \pmod 7$

$\overline{2}\, 2x \equiv \overline{2} \cdot 5 \pmod 7$

$x \equiv 4 \cdot 5 \pmod 7$

$x \equiv 20 \pmod 7$

$x \equiv 6 \pmod 7$

$x = 6$

3. a) 111 | 3 1111111 | 3 every 3 1s it's divisible by 3

Divisibility by 3

$2 \equiv 1 \bmod 3 \quad \times a_0$

$10 \equiv 1 \bmod 3 \quad \times a_1$

$\vdots \qquad \vdots$

$10^k \equiv 1 \bmod 3 \quad \times a_k$

$\Downarrow$

$a_0 \equiv a_0$

$10 a_1 \equiv a_1 \bmod 3$

$\vdots$

$10^k a_k \equiv a_k \bmod 3$

$n \equiv (a_0 + a_1 + \ldots + a_k) \bmod 3$

all digits 1, so every 3 digits will be divisible by 3

$1 \equiv 1 \pmod 6 \times a_0$

$10 \equiv 4 \pmod 6 \times a_1$

$100 \equiv 4 \pmod 6 \times a_2$

$1000 \equiv 4 \pmod 6 \times a_3$

$10000 \equiv 4 \pmod 6 \times a_4$

$\vdots$

$10^k \equiv 4 \pmod 6 \times a_k$

$n \equiv 4(a_1 + a_2 + \dots a_k) + a_0 \pmod 6$

$\sum_{i=0}^{n} 1 \equiv 4x + 1 \pmod 6$

$\sum_{i=0}^{n-1} 1 \equiv 4x \pmod 6$

Divisible by 9?
Every 9 digits

Divisible by 11?
Every other digit starting from 11 being divisible

4. $20! = m23 + r$

$20! \equiv \quad \pmod{23}$

$(n-1)! \equiv -1 \pmod n$

$22! \equiv -1 \pmod{23}$

$\overline{22}\ 22 \cdot 21 \cdot 20! \equiv -1 \pmod{23}$

$\overline{21}\ 21 \cdot 20! \equiv -22 \pmod{23}$

$20! \equiv -21 \cdot 22 \pmod{23}$

$20! \equiv 20 \cdot 23 + 2 \pmod{23}$

$20! \equiv 2 \pmod{23}$

4 - 15
5 - 13
11 - 1

11
9
7

5
3
1

h) $a_0 \times 1 \equiv 1 \pmod{11}$

$a_1 \times 10 \equiv -1 \pmod{11}$

$a_2 \times 100 \equiv 1 \pmod{11}$

$\vdots$

$a_k \times 10^k \equiv (-1)^k \pmod{11}$

$$n \equiv (a_0 - a_1 + a_2 + \ldots + (-1)^k a_k) \pmod{11}$$

$2k_1 + 2k_2 = 2(k_1 + k_2)$ * even + even = even

$2k_1 + 1 + 2k_2 + 1 = 2(k_1 + k_2 + 1)$ * odd + odd = odd

A palindrome with even number of digits has two of every digit

$$n \equiv (2a_0 - 2a_1 + 2a_2 + \ldots + 2(-1)^k a_k) \pmod{11}$$

$$n \equiv 2(a_0 - a_1 + a_2 + \ldots + (-1)^k a_k)$$

$$2(a_0 - a_1 + a_2 + \ldots + (-1)^k a_k) \pmod{2} \equiv 0$$

5. What is the remainder when 6^{325} is divided by 11?

$6 \equiv 6 \pmod{11}$

$(((6)^5)^5)^{13} \equiv ((5^5)^5)^{13} \bmod 11$

$6^5 \equiv 10 \bmod 11$

$(6^5)^5 \equiv 10^5 \pmod{11}$

$((6^5)^5)^{13} \equiv 10^{13} \pmod{11}$

$(((6^5)^5)^{13} \equiv 10 \pmod{11}$

6. $2^{p-1} + 3^{p-2} + \ldots + (p-1)^{p-1} \equiv -2 \pmod{p}$

$\Rightarrow \frac{2^p}{2} + \frac{3^p}{3} + \ldots + \frac{(p-1)^p}{p-1} \equiv -2 \pmod{p}$

$\Rightarrow$

$\varphi(p)^{\varphi(p)} \equiv -2 \pmod{p}$

$2 + 3 + \ldots + (p-1) \equiv \quad \pmod{p}$

$a^{p-1} \equiv 1 \pmod{p}$ Fermat's little theorem

$2^{p-1} \equiv 1 \pmod{p}$

$3^{p-1} \equiv 1 \pmod{p}$

$\vdots$

$(p-1)^{p-1} \equiv 1 \pmod{p}$

$2^{p-1} + 3^{p-1} + \ldots + (p-1)^{p-1} \equiv p - 1 - 1 \pmod{p}$

$\equiv p - 2 \pmod{p}$

$\equiv -2 \pmod{p}$

Theorem 6.4

7. $a^p \equiv a \pmod p$

$b^p \equiv b \pmod p$

$a^p + b^p \equiv a+b \pmod p$

$c^p \equiv a+b \pmod p$ given $a^p + b^p = c^p$

$-(a+b) + c^p \equiv 0 \pmod p$

$a+b-c^p \equiv 0 \pmod p$

$a+b-c \cdot c^{p-1} \equiv 0 \pmod p$

$c^{p-1} \equiv 1 \pmod p$ Fermat's little theorem

$a+b-c \equiv 0 \pmod p$

8. Prove that $66 \mid (n^{11} - n)$ for any positive int n

$66 = 2 \cdot 3 \cdot 11$

2: $n^{11} - n$, power preserves even and odd attribute

n is even, even + even = even

n is odd, odd + odd = even

even mod 2 = 0

3: $n^{p-1} \equiv 1 \pmod p$ Fermat's little theorem

$n^2 \equiv 1 \pmod 3$

$n^2 - 1 \equiv 0 \pmod 3$

$n^{11} - n$

$n(n^{10} - 1)$ difference of powers

$n((n^2)^5 - 1^5) = n(n^2 - 1)(n^4 - n^3 + n^2 - n + 1)$

For n not divisible by 3

For n divisible by 3:

$n = 3k$ $\quad (3k)^{11} - 3k = 3^{11}k^{11} - 3k = \underbrace{3}_{\text{divisible by 3}}(3^{10}k^{11} - k)$

11: $n^{10} \equiv 1 \pmod{11}$

$n^{10} - 1 \equiv 0 \pmod{11}$

$n^{11} - n = n(n^{10} - 1)$

For n not divisible by 11

For n divisible by 11

$n = 11k \quad (11k)^{11} - 11k = 11^{11}k^{11} - 11k = \underbrace{11}_{\text{divisible by 11}}(11^{10}k^{11} - k)$

9. Show $17^{45} \equiv 17 \pmod{45}$

$((17^3)^3)^5$

$17 \equiv 17 \pmod{45}$

$17^3 \equiv 8 \pmod{45}$

$17^9 \equiv 8^3 \pmod{45}$

$17^9 \equiv 17 \pmod{45}$

$(17^9)^5 \equiv 17^5 \pmod{45}$

$17^{45} \equiv 17 \pmod{45}$

10. Find $\varphi(11)$, $\varphi(15)$, and $\varphi(25)$

Theorem 7.2: $\varphi(11)$, 11 is prime $\Rightarrow \varphi(11) = 11 - 1 = 10$

Theorem 7.3:

$\varphi(p^2) = p^2 - p \quad \varphi(25) = \varphi(5^2) = 5^2 - 5 = 20$

Theorem 7.4: $\varphi(mn) = \varphi(m)\varphi(n)$ so,

$\varphi(15) = \varphi(5)\varphi(3)$

$= (5-1)(3-1) = 4 \cdot 2 = 8$

11: $n^{10} \equiv 1 \pmod{11}$

$n^{10} - 1 \equiv 0 \pmod{11}$

$n^{11} - n = n(n^{10} - 1)$

For n not divisible by 11

For n divisible by 11

$n = 11k \quad (11k)^{11} - 11k = 11^{11}k^{11} - 11k = \underbrace{11}_{\text{divisible by 11}}(11^{10}k^{11} - k)$

a. Show $17^{45} \equiv 17 \pmod{45}$

$((17^3)^3)^5$

$17 \equiv 17 \pmod{45}$

$17^3 \equiv 8 \pmod{45}$

$17^9 \equiv 8^3 \pmod{45}$

$17^9 \equiv 17 \pmod{45}$

$(17^9)^5 \equiv 17^5 \pmod{45}$

$17^{45} \equiv 17 \pmod{45}$

10. Find $\varphi(11)$, $\varphi(15)$, and $\varphi(25)$

Theorem 7.2: $\varphi(11)$, 11 is prime $\Rightarrow \varphi(11) = 11 - 1 = 10$

Theorem 7.3:

$\varphi(p^2) = p^2 - p \quad \varphi(25) = \varphi(5^2) = 5^2 - 5 = 20$

Theorem 7.4: $\varphi(mn) = \varphi(m)\varphi(n)$ so,

$\varphi(15) = \varphi(5)\varphi(3)$

$= (5-1)(3-1) = 4 \cdot 2 = 8$