

Solutions to MCS 425 Exercise Set #3 — Spring, 2008

Sec 3.13, exercise 12

Solution:

We need the value of $2^{10203} \pmod{101}$.

Note 101 is prime. We proved in class that, for any prime p , $u \equiv v \pmod{p-1}$ implies $a^u \equiv a^v \pmod{p}$. (This follows easily from Fermat's Little Theorem.)

$10203 \equiv 3 \pmod{100}$, so $2^{10203} \equiv 2^3 \equiv \mathbf{8} \pmod{101}$.

Sec 3.13, exercise 13

Solution:

The last two digits of 123^{562} are the value of $123^{562} \pmod{100}$.

$\phi(100) = 100(1 - 1/2)(1 - 1/5) = 40$. Since $\gcd(123, 100) = 1$, $123^{40} \equiv 1 \pmod{100}$ by Euler's Theorem, so $(123^{40})^{14} \equiv 123^{560} \equiv 1 \pmod{100}$. It follows that

$$123^{562} \equiv 123^{560+2} \equiv 123^{560} 123^2 \equiv 123^2 \equiv 23^2 \equiv 529 \equiv \mathbf{29} \pmod{100}.$$

Sec 3.13, exercise 25

Solution:

First we find integers w_1 and w_2 such: $w_1 \equiv 1 \pmod{11}$, $w_1 \equiv 0 \pmod{13}$,
 $w_2 \equiv 0 \pmod{11}$, $w_2 \equiv 1 \pmod{13}$,

$$z_1 = 143/11 = 13$$

$$z_2 = 143/13 = 11$$

$$y_1 \equiv 13^{-1} \equiv 2^{-1} \equiv 6 \pmod{11}$$

$$y_2 \equiv 11^{-1} \equiv 6 \pmod{13}$$

$$w_1 \equiv 13 \cdot 6 \equiv 78 \pmod{143}$$

$$w_2 \equiv 11 \cdot 6 \equiv 66 \pmod{143}$$

a) $x^2 \equiv 133 \pmod{143}$ is equivalent to the simultaneous congruences:

$$\text{i) } x^2 \equiv 133 \pmod{11}, \quad \text{and} \quad \text{ii) } x^2 \equiv 133 \pmod{13}.$$

$$x^2 \equiv 1 \pmod{11}$$

$$x \equiv \pm 1 \pmod{11}$$

$$x^2 \equiv 3 \pmod{13}$$

$$x \equiv \pm 4 \pmod{13}$$

by inspection. For very large moduli that are $5 \pmod{8}$, the method developed in class for this case may be applied.

$$x \equiv 1 \pmod{11} \text{ and } x \equiv 4 \pmod{13} \quad \text{implies } x \equiv 1w_1 + 4w_2 \equiv 1 \cdot 78 + 4 \cdot 66 \equiv \mathbf{56} \pmod{143}$$

$$x \equiv -1 \pmod{11} \text{ and } x \equiv 4 \pmod{13} \quad \text{implies } x \equiv -1w_1 + 4w_2 \equiv -1 \cdot 78 + 4 \cdot 66 \equiv \mathbf{43} \pmod{143}$$

The remaining two cases produce the negatives of 56 and 43.

So the solutions are $x \equiv \pm 43, \pm 56 \pmod{143}$

b) $x^2 \equiv 77 \pmod{143}$ is equivalent to the simultaneous congruences:

i) $x^2 \equiv 77 \pmod{11}$, and ii) $x^2 \equiv 77 \pmod{13}$.

$$x^2 \equiv 77 \pmod{11}$$

$$x^2 \equiv 0 \pmod{11}$$

$$x \equiv 0 \pmod{11}$$

$$x^2 \equiv 77 \pmod{13}$$

$$x^2 \equiv 12 \pmod{13}$$

$$x \equiv \pm 5 \pmod{13} \text{ by inspection. See remark above}$$

$$x \equiv 0 \pmod{11} \text{ and } x \equiv 5 \pmod{13} \text{ implies } x \equiv 0w_1 + 5w_2 \equiv 5 \cdot 66 \equiv \mathbf{44} \pmod{143}$$

$$x \equiv 0 \pmod{11} \text{ and } x \equiv -5 \pmod{13} \text{ implies } x \equiv 0w_1 - 5w_2 \equiv -5 \cdot 66 \equiv \mathbf{-44} \pmod{143}$$

So the solutions are $x \equiv \pm \mathbf{44} \pmod{143}$

Exercise F Show that 2 is a quadratic residue mod 103. (Note 103 is prime.) Find the square roots of 2 in modulus 103. (*The exercise posted on the web site had 107 in place of 103. This was an error. 2 is not a quadratic residue mod 107.*)

Solution:

$(103 - 1)/2 = 51$. To show that 2 is a quadratic residue mod 103, we need $2^{51} \equiv 1 \pmod{103}$.

$$2^{2^0} \equiv 2 \pmod{103}$$

$$2^{2^1} \equiv 2^2 \equiv 4 \pmod{103}$$

$$2^{2^2} \equiv 4^2 \equiv 16 \pmod{103}$$

$$2^{2^3} \equiv 16^2 \equiv 256 \equiv 50 \pmod{103}$$

$$2^{2^4} \equiv 50^2 \equiv 2500 \equiv 28 \pmod{103}$$

$$2^{2^5} \equiv 28^2 \equiv 784 \equiv 63 \pmod{103}$$

$$51 = (110011)_2 = 2^5 + 2^4 + 2^1 + 2^0, \text{ so } 2^{51} = 2^{2^5+2^4+2^1+2^0} = 2^{2^5} 2^{2^4} 2^{2^1} 2^{2^0} \equiv 63 \cdot 28 \cdot 4 \cdot 2 \equiv 1 \pmod{103}.$$

Since $103 \equiv 3 \pmod{4}$ and 2 is a quadratic residue mod 103, the square roots of 2 mod 103 are $\pm 2^{(103+1)/4} = \pm 2^{26} \pmod{103}$. Now $2^{26} = 2^{2^4} 2^{2^3} 2^{2^1} \equiv 28 \cdot 50 \cdot 4 \equiv 5600 \equiv 38 \pmod{103}$. So the square roots of 2 mod 53 are $\pm \mathbf{38}$.

Exercise G Show that 21 is a quadratic residue mod 37. (Note 37 is prime.) Find the square roots of 21 in modulus 37.

Solution:

$(37 - 1)/2 = 18$. To show 21 is a quadratic residue mod 37, it suffices to show that $21^{18} \equiv 1 \pmod{37}$.

$$21^{2^0} \equiv 21 \pmod{37}$$

$$21^{2^1} \equiv 21^2 \equiv 34 \pmod{37}$$

$$21^{2^2} \equiv 34^2 \equiv 9 \pmod{37}$$

$$21^{2^3} \equiv 9^2 \equiv 7 \pmod{37}$$

$$21^{2^4} \equiv 7^2 \equiv 12 \pmod{37}$$

$$18 = (10010)_2 = 2^4 + 2^1, \text{ so } 21^{18} = 21^{2^4+2^1} = 21^{2^4} 21^{2^1} \equiv 12 \cdot 34 \equiv 1 \pmod{37}.$$

$37 - 1 = 2^s m$, where $s = 2$ and $m = 9$. Since $37 \equiv 5 \pmod{8}$, 2 is a non-residue mod 37, using a result stated in class. (We could show this directly by computing $2^{18} \equiv -1 \pmod{37}$.)
 $c \equiv 2^m \equiv 2^9 \equiv 31$ is an element of order 2^s . We showed in class that when $p \equiv 1 \pmod{4}$ and $p \not\equiv 1 \pmod{8}$, the square roots of a quadratic residue $a \pmod{p}$ are either $\pm a^{(m+1)/2}$ or $\pm a^{(m+1)/2} c$. Here $(m+1)/2 = 5$. $21^5 \equiv 4 \pmod{37}$ and $21^5 31 \equiv 13 \pmod{37}$.
 $4^2 \equiv 16 \not\equiv 21 \pmod{37}$, but $13^2 \equiv 169 \equiv 21 \pmod{37}$. So the square roots of 21 mod 37 are **± 13** .

Exercise H The integer 1260 factors as $2^2 3^2 5 \cdot 7$. Compute $\varphi(1260)$ and $\lambda(1260)$.

Solution:

$$\varphi(1260) = 2^{2-1}(2-1) 3^{2-1}(3-1)(5-1)(7-1) = 2 \cdot 6 \cdot 4 \cdot 6 = \mathbf{288}$$

$$\lambda(1260) = \text{lcm}(2^{2-1}(2-1), 3^{2-1}(3-1), 5-1, 7-1) = \text{lcm}(2, 6, 4, 6) = \mathbf{12}.$$

Exercise I What is the smallest possible value of $\varphi(n) / n$ for any integer n with $2 \leq n \leq 10000$. For what value(s) of n is this minimum attained?

Solution:

We showed in class that $\varphi(n) / n < \varphi(i) / i$ for all i , $2 \leq i \leq n$, exactly when n is the product of the first k primes, for some integer k ; that is, when $n = 2$, $2 \cdot 3 = 6$, $2 \cdot 3 \cdot 5 = 30$, $2 \cdot 3 \cdot 5 \cdot 7 = 210$, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30030$, etc. Thus the smallest value of $\varphi(n) / n$ for $2 \leq n \leq 10000$ occurs first when $n = \mathbf{2310}$; this value is $(1 \cdot 2 \cdot 4 \cdot 6 \cdot 10) / (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11) = 480/2310 = \mathbf{16/77} \approx \mathbf{0.2078}$. This value is repeated whenever the one or of the primes in 2310 appears to a higher power, i.e., for $n = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = \mathbf{4620}$, $2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 = \mathbf{6930}$, and $2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = \mathbf{9240}$.