Number Theory Homework III

RDB

June 26, 2022

Exercise 1

(**a**) (5 points) Show that the last digit of n^4 in base-10 is always 1 if n is coprime with 10. [Hint: $\phi(10) = 4$. Now use Euler's theorem.]

(**b**) (5 points) Prove by induction that $5^m \equiv 5 \pmod{10}$ for all integers $m \geq 1$.

(**c**) (5 points) Prove that the last base-10 digit of $(5^k n)^4$ is 5 if n is coprime with 10 and k is any positive integer.

Solution 1

(**a**) If n is coprime with 10, then $n^4 \equiv 1 \pmod{10}$ by Euler's theorem, and the remainder mod 10 is the last digit in base-10.

(**b**) Induction. The base case is easy, and if $5^m \equiv 5 \pmod{10}$ then $5^{m+1} \equiv 25 \equiv 1 \pmod{10}$.

(**c**) By the previous two parts, we have

$$(5^k n)^4 = 5^{4k} n^4 \equiv 5 \cdot 1 \equiv 1 \pmod{10}.$$

Exercise 2

(**a**) What is the remainder of 3^{130} when divided by 11?

(**b**) What is the remainder of 8^{38} when divided by 7?

(**c**) What is the remainder of $10^{13^{100}}$ when divided by 11?

[Hint: Euler. Fermat.]

Solution 2

(**a**) (2 points) Note that $\phi(11) = 10$, and $130 = 10 \cdot 13$. Since 3 is coprime with 11, Euler's theorem states that

$$3^{130} = (3^{10})^{13} \equiv 1^13 = 1 \pmod{11}.$$

(**b**) (2 points) Note that $\phi(7) = 6$ and $38 = 6 \cdot 6 + 2$. Euler's theorem gives

$$8^{38} = 8^{6 \cdot 6+2} \equiv 8^2 \pmod{7}.$$

Then $8^2 = 64 \equiv 1 \pmod{7}$.

(**c**) (5 points) By Euler's theorem, $10^{13^{100}} \equiv 10^{13^{100} \bmod 10} \pmod{11}$ since $\gcd(10, 11) = 1$ and $\phi(11) = 10$. By Euler's theorem again, $13^{100} \equiv 13^{100 \bmod 4} = 1 \pmod{10}$ since $\gcd(13, 10) = 1$ and $\phi(10) = 4$. Therefore $13^{100} \bmod 10 = 1$, so $10^{13^{100}} \equiv 10^1 = 10 \pmod{11}$.

Another, easier way to check this is by writing $10 \equiv -1 \pmod{11}$, so that $10^{\text{odd}} \equiv -1 \equiv 10 \pmod{11}$.

Exercise 3 Euler's theorem states that $a^{\phi(n)} \equiv 1 \pmod{n}$ for every a which is coprime to n. For such an integer a, let $|a|_n$ be the *least* positive integer such that $a^{|a|_n} \equiv 1 \pmod{n}$. This is called the *multiplicative order* of a modulo n. For example,

$$\begin{aligned} 2^1 &= 2 \not\equiv 1 \pmod{7} \\ 2^2 &= 4 \not\equiv 1 \pmod{7} \\ 2^3 &= 8 \equiv 1 \pmod{7}, \end{aligned}$$

so $|2|_7 = 3$.

(**a**) Compute $|2|_n$ for $n \in \{3, 5, 7, 9, 11, 13\}$. Look these numbers up in the OEIS.

(**b**) Show that $|a|_n$ divides $\phi(n)$. [Hint: Write $\phi(n) = |a|_n k + r$ where $0 \leq r < |a|_n$. Raise a to both sides and see what happens.]

Solution 3

(**a**) (3 points, full credit if mostly right)

$$\begin{aligned}|2|_3 &= 2\\ |2|_5 &= 4\\ |2|_7 &= 3\\ |2|_9 &= 6\\ |2|_{11} &= 10\\ |2|_{13} &= 12.\end{aligned}$$

The OEIS entry is A2326.

(**b**) (5 points) If we Euclidean divide $\phi(n)$ by $|a|_n$, then we have

$$\phi(n) = |a|_n q + r$$

for some integers q and $0 \leq r < |a|_n$. By Euler's theorem we get $a^{\phi(n)} \equiv 1 \pmod{n}$, and by definition $a^{|a|_n} \equiv 1 \pmod{n}$. Therefore

$$1 \equiv a^{\phi(n)} = a^{|a|_n q + r} \equiv a^r \pmod{n}.$$

In summary,

$$a^r \equiv 1 \pmod{n},$$

and $0 \leq r < |a|_n$. Since $|a|_n$ is the *least* positive integer such that $a^{|a|_n} \equiv 1 \pmod{n}$, we cannot have $r > 0$, so $r = 0$, which shows that $|a|_n$ divides $\phi(n)$.

Exercise 4 Prove that $ab \equiv 0 \pmod{m}$ implies $b \equiv 0 \pmod{m}$ if $\gcd(a, m) = 1$.

Solution 4
The statement is just $m \mid ab$, and we proved in class that this implies $m \mid b$ if $\gcd(m, a) = 1$.

Exercise 5 Prove that if $\gcd(a, b) = 1$, and a and b both divide n, then ab divides n. [Hint: Multiply both sides of Bézout's lemma by n.]

Solution 5

By Bézout's lemma, there are integers x and y such that

$$ax + by = 1.$$

If we multiply by n, then we get

$$anx + bny = n.$$

Since b divides n, we have $n = bk$ for some integer k. Similarly, we have $n = aj$ for some integer j, so plugging these into the right places gives:

$$a(bk)x + b(aj)y = n,$$

so

$$ab(kx + jy) = n,$$

which shows that ab divides n.

Exercise 6 Fix an integer n. A subset S of $\{0, 1, 2, \ldots, n-1\}$ is *closed under multiplication mod* n provided that, if $x, y \in S$ and $xy \equiv r \pmod{n}$ with $0 \leq r < n$, then $r \in S$. For example, if $n = 10$ and $8, 2 \in S$, then $8 \cdot 2 = 16 \equiv 6 \pmod{10}$, so $6 \in S$. You could have $x = y$, so also $2 \cdot 2 = 4 \in S$.

(**a**) Find the smallest subset of $\{0, 1, 2, \ldots, 10\}$ that is closed under multiplication mod 10 and contains 2.

(**b**) Find the smallest subset of $\{0, 1, 2, \ldots, 10\}$ that is closed under multiplication mod 10 and contains 2 and 3.

Solution 6

(**a**) (5 points) Let S be the smallest subset. Since $2 \in S$, we must have $2^2 = 4 \in S$, which then gives $2 \cdot 4 = 8 \in S$, and also $4^2 = 16 \equiv 6 \in S$. Thus S contains at least $\{2, 4, 6, 8\}$, and conversely this set is closed under multiplication. Therefore $S = \{2, 4, 6, 8\}$.

(**b**) (5 points) Let J be the smallest subjset. Since $2 \in S$, from the previous part J must contain at least $\{2, 4, 6, 8\}$. But it also must contain $9 = 3^2$ and $7 \equiv 3 \cdot 9 \pmod{10}$. Then $1 \equiv 3 \cdot 7 \pmod{10}$ is also in there, so J contains at least

$$\{1, 2, 3, 4, 6, 7, 8, 9\}.$$

Conversely this set is closed under multiplication, so J equals it exactly.