27 Jul '21
Emilie

FERMAT'S LITTLE THEOREM QNS.

① $3^{31} \bmod 7$

$a^{(p-1)} \equiv 1 \bmod p \rightarrow 3^6 \equiv 1 \bmod 7$

$3^{31} \equiv (3^6)^5 \cdot (3) \equiv 1^5 \cdot (3) \equiv 3 \bmod 7$

② $2^{35} \bmod 7$

by Fermat's little theorem, $2^6 \equiv 1 \bmod 7$

$2^{35} \equiv (2^6)^5 \cdot (2)^5 \equiv 1 \cdot 32 \equiv 32 \equiv 4 \bmod 7$

③ $128^{129} \bmod 17$

$128^{16} \equiv 1 \bmod 17$

$128 \bmod 17 = 9 \rightarrow 9^{16} \equiv 1 \bmod 17$

$128^{129} \equiv 9^{129} \equiv (9^{16})^8 \cdot (9) \equiv 1^8 \cdot 9 \equiv 9 \bmod 17$

④ $2^{1000} \bmod 13$

$2^{12} \equiv 1 \bmod 13$

$2^{1000} \equiv (2^{12})^{83} \cdot 2^4 \equiv 2^4 \equiv 16 \equiv 3 \bmod 13$

⑤ $29^{25} \bmod 11$

$29 \equiv 7 \bmod 11$

$7^{10} \equiv 1 \bmod 11$

$29^{25} \equiv 7^{25} \equiv (7^{10})^2 \cdot 7^5 \equiv 7 \cdot 7^2 \cdot 7^2 \bmod 11$

$7^2 = 49 \equiv 5 \bmod 11$

$7 \cdot 5 \cdot 5 = 175 \equiv 10 \bmod 11$

⑥ $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \bmod 7$

$2^6 \equiv 3^6 \equiv 4^6 \equiv 5^6 \equiv 6^6 \equiv 1 \bmod 7$

$2^{20} \equiv (2^6)^3 \cdot 2^2 \equiv 4 \bmod 7$

$3^{30} \equiv (3^6)^5 \equiv 1 \bmod 7$

$4^{40} \equiv (4^6)^6 \cdot (4^4) \equiv 256 \equiv 4 \bmod 7$

$5^{50} \equiv (5^6)^8 \cdot 5^2 \equiv 25 \equiv 4 \bmod 7$

$6^{60} \equiv (6^6)^{10} \equiv 1 \bmod 7$

⑥ CONT. $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \equiv 4+1+4+4+1 \equiv 14 \equiv 0 \bmod 7$

! ⑦ $a_1 = 4,\ a_n = 4^{a_{n-1}},\ n>1,\ a_{100}$

$4^6 \equiv 1 \bmod 7$

$4^1 \equiv 4^2 \equiv 4^3 \equiv 4^4 \equiv \ldots\ 4 \bmod 6$

$4^{a_n} \equiv 4 \bmod 6$ for all $n>1$, so $a_n \equiv 4 \bmod 6$

$a_{100} = 4^{a_{99}} \equiv 4^4(4^6)^x \equiv 4^4 = 256 \equiv 4 \bmod 7$

⑧ $x^{103} \equiv 4 \bmod 11$

$x^{10} \equiv 1 \bmod 11$

$x^{103} \equiv (x^{10})^{10} \cdot x^3 \equiv x^3 \equiv 4 \bmod 11$

$x=1,\ x^3=1,\ != 4 \bmod 11$

$x=2,\ x^3=8,\ != 4 \bmod 11$

$x=3,\ x^3=27,\ != 4 \bmod 11$

$x=4,\ x^3=64,\ != 4 \bmod 11$

$x=5,\ x^3=125 \equiv 4 \bmod 11 \rightarrow x=5$

⑨ $x^{86} \equiv 6 \bmod 29$

$x^{28} \equiv 1 \bmod 29$

$x^{86} \equiv (x^{28})^3 \cdot x^2 \equiv x^2 \equiv 6 \bmod 29$

(try all x from $x=0$ to $x=29$)

$x = 8, 21$

! ⑩ periods of sequence $x, x^2, x^3 \bmod 13$

$x^{12} \equiv 1 \bmod 13$

- periods of sequence $= \{1, 2, 3, 4, 6, 12\}$
  - cycle length 1 $\Rightarrow x = 0, 1, 13$
  - cycle length 12 $\Rightarrow x = 2$
  - cycle length 2 $\Rightarrow x = 2^{12/2} = 2^6 = 64 \equiv 12 \bmod 13$
  - cycle length 3 $\Rightarrow x = 2^{12/3} = 2^4 = 16 \equiv 3 \bmod 13$
  - cycle length 4 $\Rightarrow x = 2^{12/4} = 2^3 \equiv 8 \bmod 13$
  - cycle length 6 $\Rightarrow x = 2^{12/6} = 2^2 \equiv 4 \bmod 13$
- confused about how they got x for cycle length 2 from cycle length 12?

(11) $10^{10^{100}}$ mod 7

- use euler's theorem $\to a^{\varphi n} \equiv 1 \bmod n$ for first part

$\left[10^{\left[10^{100}\right]_{\bmod \Phi(7)}}\right]_{\bmod 7}$

$\Phi(7) = (7-1) = 6$

$\Phi(\Phi(7)) = \#\{1,5\} = 2$

10^{100} mod 6

$10^2 = 100 \equiv 4 \bmod 6 \to 10^k \equiv 4 \bmod 6$

$10^4 \equiv 4 \bmod 7$ (hand calculate)

- 4 days from sunday, so thursday

!(12) p, q are distinct primes, $a^p \equiv a \bmod p$, $a^q \equiv a \bmod q$

prove $a^{pq} \equiv a \bmod (pq)$

$(a^p)^q \equiv a^q \equiv a \bmod p$

$(a^q)^p \equiv a^p \equiv a \bmod q$

$a^{pq} = px + a = qy + a \to px = qy$

$x = qn,\ y = pn$ for some n

$a^{pq} = p(qn) + a = q(pn) + a$

$a^{pq} \equiv a \bmod pq$

!(13) $2^{2^x+1} + 2 \bmod 17 = 0$, find x

let 2^x+1 be a

$2^a + 2 \equiv 0 \bmod 17$

$2^a \equiv -2 \equiv 15 \equiv 32 \bmod 17$

$a = 5,\ 2^5 = 32$

- forgot to consider modulo when calculating

$2^x + 1 \equiv 5 \bmod 8 \to 8$ is cycle length for powers of 2

$2^x \equiv 4 \bmod 8$

$x = 2$

- I followed through the rest but couldn't do them on my own