Feb. 25th

THING TO KNOW REALLY WELL:

→ Induction
→ Fermat Theorem / EULER / WILSON
  * COMPUTATIONS
→ RSA { ENCRYPT, DECRYPT, SETUP

RATIONALS
PRIMES

REDO HOMEWORK
LOOK @ LECTURES
@ TEXT BOOK

Compute $3^{3^{100}} \bmod 100$ (i.e. finding its last 2 digits)

→ "simplify the exponent"

know $3^{\varphi(100)} \equiv 1 \bmod 100$ by Euler's Thm since $\gcd(3, 100)=1$

We reduce $3^{100} \bmod \varphi(100)$

$\varphi(100) = 2^2 \cdot 5^2 = 2^2-2^1)(5^2-5^1) = 2 \cdot 20 = 40$

$3^{100} \bmod \varphi(100) \equiv 3^{100} \bmod 40 \equiv (3^4)^{25} \bmod 40 \equiv (81)^{25} \bmod 40$

$\equiv 1 \bmod 40$

$3^{100} = k\varphi(100) + 1, \quad k \in \mathbb{Z}$

$3^{k\varphi(100)+1} \bmod 100 \equiv 1^k \cdot 3 \bmod 100 = 3 \bmod 100$

so the last 2 digits are 03.

Claim: $\varphi(p_1^{k_1} p_2^{k_2} p_3^{k_3}) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})(p_3^{k_3} - p_3^{k_3-1})$

From tutorial $\gcd(m,n)=1 \Rightarrow \varphi(m,n) = \varphi(m)\varphi(n)$

so — $\varphi(p_1^{k_1} p_2^{k_2} p_3^{k_3}) = \varphi(p_1^{k_1})\varphi(p_2^{k_2})\varphi(p_3^{k_3})$

LEMMA: $\varphi(p^k) = p^k - p^{k-1}$

Find the remainder $(9! \times 16 + 4311)^{8603} \bmod 11$

$\equiv (9! \cdot 5 + 10)^{8603}$

COR $a^p \equiv a \bmod p$

$\equiv (9! \cdot 5 + 10)^{8600+3}$

$\equiv (-10 \cdot 5 + 10)^{8603}$

$\equiv (-4 \cdot 10)^{8603}$

$10 \cdot 10 \equiv 100 \equiv 9 \cdot 11 + 1 \equiv 1 \bmod 11$

$10 \cdot 10! \equiv 10 \cdot 10 \cdot 9! \equiv -1 \cdot 10 \bmod 11$

$\equiv ((-4)\cdot(-1))^{8003}$

$\equiv 4^{800\cdot 10+3}$

$\equiv 4^3 \bmod 11$ by Fermat Theorem $\gcd(4, 11)=1$

Claim: All people are the same age.

By induction on size of sets of people

let $|S|=1$

certainly $x, y \in S \Rightarrow age(x)=age(y)$

Suppose the claim holds for sets of people of size n.

Let $|S|=n+1$

Now take $S=X\cup Y$ where $|(X\cap Y)|=1$ and $|X|=n$, $|Y|=n$

Write $X\cap Y=\{z\}$
$x\in X \Rightarrow age(x)=age(z)$
$y\in Y \Rightarrow age(y)=age(z)$

Thus $x,y\in S \Rightarrow age(x)=age(y)$

Claim: $20^{2/5}$ is irrational

Sps it is rational $20^{2/5}=p/q$ for $p, q \in \mathbb{Z}$, $\gcd(p, q)=1$

$(20^{2/5})^5 = p^5/q^5$

$\Rightarrow 20^2 = p^5/q^5 \Rightarrow 20^2 q^5 = p^5$

$\Rightarrow p$ even

Let $p=2n$

$2^4 5^2 q^5 = 20^2 q^5 = (2n)^5 = 2^5 n^5$

by canonical factorization we have ≥ 5 copies of 2 on RHS $\Rightarrow$ one copy of 2 occurs in q.