$\varphi(n) = \#$ of integers $0<a<n$, $(a,n)=1$. RRS (mod n) = set of $\varphi(n)$ integers s.t. $\forall x \in RRS$, $(x,n)=1$, $x \not\equiv y \bmod n$ $\forall y \neq x \in RRS$. Ex: $n=8 \to \{1,3,5,7\}$.

Euler's Theorem: $(a,m)=1$, $a^{\varphi(m)} \equiv 1 \pmod m$, $a\in\mathbb{Z}$, $m\geq 1$ $\Rightarrow$ $a^{\varphi(m)-1} = a^{-1} \pmod m$. Note: p prime $\Rightarrow \varphi(p-1)=p-1 \Rightarrow a^{p-1}\equiv 1 \pmod p$. $\to ax\equiv b \bmod m$, $(a,m)=1$ $\to x \equiv a^{\varphi(m)-1}\cdot b \pmod m$

Properties of $\varphi(m)$: Assume p prime, $a>1$. 1) $\varphi(p^a)=p^{a-1}(p-1)$ 2) $m=m_1m_2$, $(m_1,m_2)=1 \Rightarrow \varphi(m)=\varphi(m_1)\varphi(m_2)$. $\to \varphi(n)=\varphi(p_1^{d_1})\cdots\varphi(p_r^{d_r}) = p_1^{d_1-1}(p_1-1)\cdots p_r^{d_r-1}\ldots$ 3) $\varphi(n)$ even $\forall n>2$.

Theorem: $ax\equiv b \bmod m$: Let $d:=(a,m)$. 1) $d\nmid b \Rightarrow$ no solutions 2) $d\mid b \Rightarrow d$ solutions: $x=x_0+\frac{m}{d}t \pmod m$, $t=0,\ldots,d-1$. **Euclidean Algorithm:** $a=bq+r$, $0\leq r<b$. $(a,b)=(b,r)=(r,r_2)$

Divisibility: 1) $a\mid b \wedge b\mid c \Rightarrow a\mid c$ 2) $a\mid b,c \Rightarrow a\mid bx+cy$ 3) $a\mid b \Rightarrow ma\mid mb$. **Bezout:** $(a,d)=d \Leftrightarrow ax+by=d$. **Euclid's Lemma:** p prime, $p\mid ab \Rightarrow p\mid a$ or $p\mid b$.

Theorem: $ax+by=c$: Let $d:=(a,b)$ 1) $d\nmid c \Rightarrow$ no solutions 2) $d\mid c \Rightarrow \begin{cases} x=x_0+(b/d)t \\ y=y_0-(a/d)t \end{cases}$ **Fundamental Theorem of Arithmetic:** $n\in\mathbb{Z}$, $n>1 \Rightarrow n=p_1^{d_1}\cdots p_r^{d_r}$, p_i prime, $d_i\in\mathbb{Z}^+$.

Dirichlet's Theorem: Fix $a,b\in\mathbb{Z}^+$, $(a,b)=1 \Rightarrow \exists$ infinitely many primes $ak+b$. **FLT:** p prime, $p\nmid a \Rightarrow a^{p-1}\equiv 1 \bmod p$. 1) $a\in\mathbb{Z}^+ \Rightarrow a^p\equiv a \bmod p$ 2) $a^{b^c} \bmod p \to$ examine $b^c \bmod p-1$.

Wilson's Theorem: If $(a,p)=1$, then $\exists a^{-1} \bmod p$. 1) p prime $\Rightarrow (p-1)!\equiv -1 \bmod p$ 2) $n\geq 2 \wedge (n-1)!\equiv -1 \bmod n \Rightarrow n$ prime. **Complete Residue System:** $\{[0]_m,\ldots,[m-1]_m\} \longleftrightarrow \mathbb{Z}/m\mathbb{Z}$

CRS: $\{r_1,\ldots,r_m\}$ is CRS $\wedge$ $(a,m)=1 \Rightarrow \{ar_1,\ldots,ar_m\}$ also CRS. **Invertibility** ($ax\equiv 1 \bmod m$) Let $d:=(a,m)$. 1) $d\neq 1 \Rightarrow$ no solutions 2) $d=1 \Rightarrow \exists$ unique solution mod m.

Modular Arithmetic: 1) $a\equiv b \bmod m \Rightarrow b^k\equiv a^k \bmod m$, $k\in\mathbb{Z}$ 2) transitivity holds 3) $\begin{matrix} a\equiv b \bmod m \\ c\equiv d \bmod m\end{matrix} \Rightarrow a+c\equiv b+d \bmod m$ 4) $d\mid m \wedge a\equiv b \bmod m \Rightarrow a\equiv b \bmod d$ 5) $c>0 \wedge a\equiv b \bmod m \Rightarrow ac\equiv bc \bmod m$ 6) $ac\equiv bc \bmod m \Rightarrow a\equiv b \bmod \frac{m}{(c,m)}$

Theorem A: 1) $ax\equiv ay \bmod m \Leftrightarrow x\equiv y \bmod \frac{m}{(a,m)}$ 2) $ax\equiv ay \bmod m \wedge (a,m)=1 \Rightarrow x\equiv y \bmod m$ 3) If $x\equiv y \bmod m_i$, $1\leq i\leq n$, then $\begin{cases} x\equiv y \bmod m_1 \\ x\equiv y \bmod m_n\end{cases} \Leftrightarrow x\equiv y \bmod \operatorname{lcm}(m_1,\ldots,m_n)$

Chinese Remainder Theorem: If $(m_i,m_j)=1$, $\forall i\neq j$, then $\begin{cases} x\equiv a_1 \bmod m_1 \\ \vdots \\ x\equiv a_r \bmod m_r\end{cases}$ $\exists!$ solution $x_0 \bmod m^{m_1\cdots m_r}$: $x_0=\frac{m}{m_1}b_1a_1+\cdots+\frac{m}{m_r}b_ra_r \bmod m$, where $b_i\left(\frac{m}{m_i}\right)\equiv 1 \bmod m_i$.

Primitive Roots: Let $m>1$, $(g,m)=1$. If $\operatorname{ord}_m g=\varphi(m) \to g$ is primitive root (mod m). **Primitive Roots:** Let g be a primitive root mod m. Then 1) $\{1,g,\ldots,g^{\varphi(m)-1}\}$ is RRS. 2) $g^ig^j=g^{(i+j) \bmod \varphi(m)} \bmod m$

Prime Primitive Roots: 1) Every prime p has a primitive root 2) p odd $\to \exists\varphi(p-1)$ primitive roots (mod p) **Powers of Prim Roots:** r primitive root mod $m^?$, then r^n prim root mod $m \Leftrightarrow (n,\varphi(m))=1$

Primitive Root Theorem: $\exists$ primitive root mod $m \Leftrightarrow m\in\{2,4,p^n,2p^n\}$, $p>2$ prime. Given a primitive root g mod p (p-odd prime), then $\operatorname{ord}_{p^2} g\in\{p-1,p(p-1)\}$. Then:
1) Either g or $g+p$ is a primitive root (mod p^2) 2) A primitive root mod p^2 is a primitive root mod p^n, $n\geq 2$. 3) If h is a primitive root mod p^n, either $h+p^n$ or h (whichever is odd) is prim root (mod $2p^n$)
4) Given g a primitive root mod n: g^k is a primitive root mod $n \Leftrightarrow (k,\varphi(n))=1$ **Theorem:** $m=m_1m_2$, $m_1,m_2>2 \Rightarrow$ no primitive roots mod m. **Funny index exponent:** $g^{\operatorname{ind}_g a}\equiv a \bmod m$

Indices: Let $m\in\mathbb{Z}^+$ with primitive root g. If $a\in\mathbb{Z}^+$, $(a,m)=1$, then $\exists! x\in\mathbb{Z}$, $1\leq x\leq\varphi(m) \wedge g^x\equiv a \bmod m$, called the index of a to the base g mod m. $a\equiv b \bmod m \Leftrightarrow \operatorname{ind}_g a\equiv \operatorname{ind}_g b \bmod m$

Indices Properties: Let $m\in\mathbb{Z}^+$ with primitive root g, $(a,m)=(b,m)=1$. Then 1) $\operatorname{ind}_g 1\equiv 0 \pmod{\varphi(m)}$ 2) $\operatorname{ind}_g(ab)\equiv \operatorname{ind}_g a+\operatorname{ind}_g b \pmod{\varphi(m)}$ 3) $\operatorname{ind}_g(a^k)\equiv k\cdot\operatorname{ind}_g a \pmod{\varphi(m)}$ $\forall k\in\mathbb{Z}^+$

Index Arithmetic: $x^k\equiv a \bmod m$, let $(a,m)=1$, g be primitive root mod m. Then 1) $g^{k\cdot\operatorname{ind}_g x}\equiv g^{\operatorname{ind}_g a} \bmod m$ 2) $k\cdot\operatorname{ind}_g x\equiv\operatorname{ind}_g a \pmod{\varphi(m)}$. Let $d=(k,\varphi(m))$. $d\nmid \operatorname{ind}_g a \Rightarrow k\cdot\operatorname{ind}_g x\equiv\operatorname{ind}_g a \bmod\varphi(m) \to$ no solutions; $d\mid\operatorname{ind}_g a \Rightarrow k\cdot\operatorname{ind}_g x\equiv\operatorname{ind}_g a \bmod\varphi(m) \to d$ solutions
$d\mid\operatorname{ind}_g a \Leftrightarrow a^{\varphi(m)/d}\equiv 1 \bmod m$. **Solvability:** $x^n\equiv a \bmod m$ is solvable $\Leftrightarrow a^{\varphi(m)/d}\equiv 1 \bmod m$, $d=(n,\varphi(m))$. **Equivalence of Indices:** $(a,m)=(b,m)=1 \Rightarrow a\equiv b \bmod m \Leftrightarrow \operatorname{ind}_g a=\operatorname{ind}_g b$

Hensel's Lemma (Singular Roots): $f(a)=0 \pmod{p^i} \wedge [(f'(a),p)\neq 1$ or $p\mid f'(a)] \Rightarrow f(a+p^it)\equiv f(a) \pmod{p^{i+1}} \Rightarrow$ 1) $f(a)\equiv 0 \pmod{p^{i+1}} \Rightarrow a \bmod p^i$ lifts to p distinct roots $a+tp^i$, $0\leq t\leq p-1$.
2) $f(a)\not\equiv 0 \bmod p^{i+1} \Rightarrow$ none of the lifts are roots mod p^{i+1} **Hensel's Lemma (Non-singular):** $f(a)\equiv 0 \bmod p^i$, $(f'(a),p)=1 \Rightarrow \exists!\, t \bmod p$ s.t.

Solve $f(x)\equiv 0 \bmod m$: If $m=m_1m_2$, $(m_1,m_2)=1$, then $(\#$ of solutions to $f(x)\equiv 0 \bmod m)=N(m)=N(m_1)\cdot N(m_2)$. *Use CRT to solve* $f(a+tp^i)\equiv 0 \bmod p^{i+1}$. To find: $tf'(a)\equiv -\frac{f(a)}{p^i} \bmod p$.

Lagrange's Theorem: Let p be prime, $f(x)=a_0+a_1x+\cdots+a_nx^n$, $a_i\in\mathbb{Z}$ and $(a_i,p)=1$ for some i. Then $f(x)\equiv 0 \bmod p$ has $\leq n$ solutions mod p. $\operatorname{ord}_m a\mid\varphi(m)$

Order of an element: Define $\operatorname{ord}_m a :=$ smallest $n\in\mathbb{Z}^+$ s.t. $a^n\equiv 1 \bmod m$. Random order shit: $(a,m)=1$, $a\neq 0$, $m>1 \Rightarrow$ 1) $a^x\equiv 1 \bmod m \Leftrightarrow \operatorname{ord}_m a\mid x$. 2) $a^{\varphi(m)}\equiv 1 \bmod m$
3) $a\equiv b \bmod m \Rightarrow \operatorname{ord}_m a=\operatorname{ord}_m b$ 4) $a^k\equiv a^l \Leftrightarrow k\equiv l \bmod \varphi(m)$.

Arithmetic Functions: $f:\mathbb{N}\to\mathbb{R}$. 1) $\tau(n)=\sum_{d\mid n}1=\#$ of positive divisors of n 2) $\sigma(n)=\sum_{d\mid n}d$ 3) $\sigma_k(n)=\sum_{d\mid n}d^k$ 4) $\varphi(n)=\sum_{\substack{(a,n)=1 \\ 1\leq a\leq n}}1$

Multiplicity of $F(n)$: $f:\mathbb{N}\to\mathbb{R}$ multiplicative $\Rightarrow F(n):=\sum_{d\mid n}f(d)$ is multiplicative. **Multiplicative:** $f(mn)=f(m)f(n)$ $\begin{cases}\forall (m,n)=1 \to \text{multiplicative} \\ \forall m,n \to \text{completely multiplicative}\end{cases}$ $\hookrightarrow$ hint: $f:\mathbb{N}\to\mathbb{R}$ multiplicative, compute $f(p_i^{d_i})$ instead ($n=\prod p_i^{d_i}$)

Mobius Function: $\mu=\begin{cases}1 & n=1 \\ 0 & p^2\mid n \\ (-1)^r & n=p_1\cdots p_r\end{cases}$ **Mobius Mult:** $\mu:\mathbb{N}\to\mathbb{R}$ is multiplicative $\Rightarrow \sum_{d\mid n}\mu(d)=\begin{cases}0 & n=1 \\ 1 & n>1\end{cases}$

Mobius Inversion Function: $g(n)=\sum_{d\mid n}f(d) \Leftrightarrow f(n)=\sum_{d\mid n}\mu(d)g\left(\frac{n}{d}\right)=\sum_{d\mid n}\mu(n/d)g(d)$

Check for prim. roots by finding $d\mid\varphi(n)$: $\varphi(25)=20 \Rightarrow \operatorname{ord}_{25}2\equiv 1,2,4,5,10,20$ $\hookrightarrow 2^1,2^2,2^4,2^5,2^{10}\not\equiv 1 \bmod 25$

Ex: $x^{12}\equiv 16 \bmod 17$: 3 is prim. root $\to 3^{12\operatorname{ind}_3 x}\equiv 3^{\operatorname{ind}_3 16} \bmod 17 \to 12\operatorname{ind}_3 x\equiv\operatorname{ind}_3 16 \bmod 16 \to 12\operatorname{ind}_3 x\equiv 8 \bmod 16 \to 3\operatorname{ind}_3 x\equiv 2 \bmod 4 \to \operatorname{ind}_3 x\equiv 2 \bmod 4 \to 3^i\equiv x \bmod 17$, $i=2,6,10,14 \bmod 16$ $\hookrightarrow x\equiv 3^2,3^6,3^{10},3^{14} \bmod 17$

Ex: $7^x\equiv 6 \bmod 17$: $3^{x\operatorname{ind}_3 7}\equiv 3^{\operatorname{ind}_3 6} \bmod 17 \Rightarrow x\operatorname{ind}_3 7\equiv\operatorname{ind}_3 6 \bmod 16 \to 11x\equiv 15 \bmod 16 \to x\equiv 13 \bmod 16$. | a is square mod 11: $x^2\equiv a \bmod 11 \Leftrightarrow a^{10/2}\equiv 1 \bmod 11 \to a\equiv 1$ | 2 is prim root mod 11 $\hookrightarrow$ other sols of form 2^j, $\operatorname{ord}(2^j)=\frac{10}{(j,10)}=5$ $\hookrightarrow j=2,4,6,8$

MT1P1: 1) Find all pos. int. solutions to $97x+98y=1000$: $(97,98)\to x_0'=-1$, $y_0'=1$ is solution to $97x+98y=1$. $\Rightarrow x_0=-1000$, $y_0=1000$ is solution to $97x+98y=1000$. General solution is $\begin{cases}x=-1000t+98t \\ y=1000(-97t\end{cases}$
We want $x,y>0$, so $x=-1000+98t>0 \Rightarrow 98t>1000$, $t>10$. $y=1000-97t>0 \Rightarrow 97t<10$, $t<10$ $\therefore \nexists$ solutions >0. 2) Show if $(x,3)=1$ and $(y,3)=1$, then x^2+y^2 cannot be a perfect square.
$(x,3)=1 \Rightarrow x\not\equiv 0 \bmod 3 \Rightarrow x,y\equiv 1,2 \bmod 3$. $\Rightarrow x^2\equiv y^2\equiv 1 \bmod 3$. $\Rightarrow x^2+y^2\equiv 2 \bmod 3$. But $x^2 \bmod 3\in\{0,1\}$ ∎ 3) a) Given that $(a,4)=2$ and $(b,4)=2$, prove that $(a+b,4)=4$.
Suppose $(a,4)=2$, $(b,4)=2$. $\Rightarrow 2\mid a,b$ but $4\nmid a,b$. $\Rightarrow a=2a_0$, $b=2b_0$, a_0,b_0 odd. Then $a+b=2(\underbrace{a_0+b_0}_{\text{even}}) \to 4\mid a+b$. b) Compute (n,n^2+n+1): Suppose $d\mid n$, $d\mid n^2+n+1$. Then
$d\mid(n^2+n+1)-n(n+1)=1$. ∎ 4) Show if $n\in\mathbb{Z}^+$ then $5^n\equiv 1+4n \bmod 16$: Suppose $5^n\equiv 1+4n \bmod 16$ holds for some $n\in\mathbb{N}$. Then $5^{n+1}=5\cdot 5^n\equiv 5(1+4n) \bmod 16\equiv 5+4n \bmod 16$ $\left(1+4(1+n)\right)$. ∎

5) Let p be prime. Find the largest power of p that divides $(p^2-1)!$: The factors of $(p^2-1)!$ that divide p are $\overbrace{p,2p,\ldots,p(p-1)}^{S}$, and $p^2\nmid x\in S$. Thus $p^{p-1}\mid(p^2-1)! \Rightarrow p-1$ largest power dividing $(p^2-1)!$

MT1P2: 1) Find all x,y such that $250x+237y=1$: (1) $\boxed{250}=\boxed{237}\cdot 1+\boxed{13}$ (2) $\boxed{237}=\boxed{13}\cdot 18+\boxed{3}$ (3) $\boxed{13}=\boxed{3}\cdot 4+\boxed{1}$ $\Rightarrow (237,250)=1$. We have (1) $r_1=a-b$
(2) $r_2=b-18r_1=\cdots=-18a+19b$ (3) $r_3=r_1-4r_2=\cdots=73a-77b$. Thus $x_0=73$, $y_0=-77$ is an integer solution. The general solution is $\begin{cases}x=73+237t \\ y=-77-250t\end{cases}$, $t\in\mathbb{Z}$.

2) Solve $\begin{cases}x\equiv 2 \bmod 14 \\ x\equiv 16 \bmod 21 \\ x\equiv 10 \bmod 30\end{cases}$: Theorem A $\Rightarrow$ $x\equiv 2 \bmod 14 \Leftrightarrow \begin{cases}x\equiv 0 \bmod 2 \\ x\equiv 2 \bmod 7\end{cases}$, $x\equiv 16 \bmod 21 \Leftrightarrow \begin{cases}x\equiv 1 \bmod 3 \\ x\equiv 2 \bmod 7\end{cases}$, $x\equiv 10 \bmod 30 \Leftrightarrow \begin{cases}x\equiv 0 \bmod 2 \\ x\equiv 0 \bmod 5 \\ x\equiv 1 \bmod 3\end{cases}$. Combining the distinct equations, we get: $\begin{cases}x\equiv 0 \bmod 2 \\ x\equiv 2 \bmod 7 \\ x\equiv 1 \bmod 3 \\ x\equiv 0 \bmod 5\end{cases}$ $\begin{matrix}m_1=2 & a_1=0 \\ m_2=7 & a_2=2 \\ m_3=3 & a_3=1 \\ m_4=5 & a_4=0\end{matrix}$ $\to x=\frac{m}{m_1}a_1b_1+\cdots+\frac{m}{m_4}a_4b_4=0+(2\cdot 3\cdot 5)\cdot 2\cdot b_2+(2\cdot 7\cdot 5)\cdot 1\cdot b_3+0=310 \bmod 210\equiv 100 \bmod 210$. (inv. of $2\cdot 3\cdot 5$ mod 7 $\to\equiv 2$ mod 7; inv. of $2\cdot 7\cdot 5$ mod 3 $\to\equiv 1$ mod 3)

3) Does there exist an integer n such that $3\mid n^2+n+2$? Suppose $\exists n\in\mathbb{Z}$ s.t. $3\mid n^2+n+2$. $\Rightarrow n^2+n+2\equiv 0 \bmod 3$. Use cases to find no. 4) Let $n\geq 2$. Show if $d\mid n^2+1$ and $d\mid(n+1)^2+1$, then $d=1$ or $d=5$: Note that $n^2+2n+2-(n^2+1)=2n+1 \Rightarrow d\mid 2n+1 \Rightarrow d\mid(2n+1)^2$. Then $d\mid 2n+1$, $d\mid 4n+7 \Rightarrow d\mid 5$ ∎

5) Determine the last digit of 323^{700}: WTF: $323^{700} \bmod 10$. $323\equiv 3 \bmod 10 \Rightarrow 323^{700}\equiv 3^{700} \bmod 10$. But $3^4=81\equiv 1 \bmod 10$ and $700=4\cdot 175$. $\Rightarrow 1$

MT2P1: 1) a) Compute the last two digits of 2393^{6642}: Note that $2393\equiv 93 \bmod 100$, so $2393^{6642}\equiv 93^{6642} \bmod 100$. Since $(93,100)=1$, we can apply Euler's theorem: $\varphi(100)=\varphi(4)\cdot\varphi(25)=2\cdot 20=40 \to 93^{40}\equiv 1 \bmod 100$. $6642=166\cdot 40+2 \Rightarrow 93^{6642}\equiv(93^{40})^{166}\cdot 93^2\equiv 93^2\equiv 49 \bmod 100$ b) For which integers $n>0$ is $\varphi(n)=6$? Consider p prime with $p\mid n$. Then $p-1\mid\varphi(n) \Rightarrow p-1=1,2,\cancel{3},6 \Rightarrow p=2,3,7$. Case 1: $7\mid n$. $n=7^a\cdot k$, $(k,7)=1$. $\varphi(n)=7^{a-1}\cdot 6\cdot\varphi(k)=6 \Rightarrow a=1$, $\varphi(k)=1$
$\Rightarrow k=1,2 \Rightarrow n=7,14$. Case 2: $7\nmid n$. Then $n=2^a3^b$, $a,b\geq 0$. Need $b\geq 2$, else $3\nmid\varphi(n)$. Then $\varphi(n)=\varphi(2^a)\varphi(3^b)=\varphi(2^a)3^{b-1}\cdot 2=6 \Rightarrow b=2$, $a=0,1 \Rightarrow n=9,18$.

2) Let p be an odd prime. Show $\sum_{i=1}^{p-1}i^p\equiv 0 \bmod p$: FLT $\Rightarrow i^p\equiv i \bmod p \Rightarrow \sum i^p\equiv\sum i=\frac{p(p-1)}{2} \bmod p$. p odd $\Rightarrow \frac{p-1}{2}\in\mathbb{Z} \Rightarrow p\mid p\left(\frac{p-1}{2}\right) \Rightarrow p\left(\frac{p-1}{2}\right)\equiv 0 \bmod p$ ∎

3) Find all solutions of $\overbrace{x^2+6x-31}^{p(x)} \equiv 0 \bmod 72$: $p(x) \equiv 0 \bmod 8$ has two sols: $1, 5 \bmod 8$; $p(x) \equiv 0 \bmod 9$ has two: $4, 8 \bmod 9$ $\Rightarrow \exists$ 4 sols mod 72 ① $\begin{cases} x \equiv 1 \bmod 8 \\ x \equiv 4 \bmod 9 \end{cases}$ ... ② $\begin{cases} x \equiv 1 \bmod 8 \\ x \equiv 8 \bmod 9 \end{cases}$ ...

4) Find the number of solutions to the congruence $x^2 \equiv 9 \bmod 3 \cdot 11^2 \cdot 13^3$: Need to solve $\begin{cases} x^2 \equiv 9 \bmod 3 \\ x^2 \equiv 9 \bmod 11^2 \\ x^2 \equiv 9 \bmod 13^3 \end{cases}$. 1) $x^2 \equiv 9 \bmod 3 \Leftrightarrow x^2 \equiv 0 \bmod 3 \Rightarrow$ one solution

2) $x^2 \equiv 9 \bmod 11$ has two solutions: $x \equiv 3, 8 \bmod 11$. (Lagrange $\rightarrow \exists \le 2$ sol) $f(x) = x^2 - 9$, $f'(x) = 2x$, $11 \nmid f'(3)$, $11 \nmid f'(8)$ $\rightarrow$ 3, 8 both non-singular $\rightarrow$ lift to unique root $\rightarrow$ two sols mod 11^2

3) $x^2 \equiv 9 \bmod 13$ has two nonsingular roots $\rightarrow$ two sols mod 13^3. $\rightarrow N(3 \cdot 11^2 \cdot 13^3) = N(3) \cdot N(11^2) \cdot N(13^3) = 1 \cdot 2 \cdot 2 = 4$

5) Show if $b \in \mathbb{Z}, b > 1$, $n > 1$ odd, then $(b^n - 1, b^l + 1) \le 2$: Suppose $m > 2$ s.t. $m \mid b^n - 1 \wedge m \mid b^l + 1 \Rightarrow b^n \equiv 1 \bmod m \wedge b^l \equiv -1 \bmod m \Rightarrow b^{2l} \equiv 1 \bmod m$. Then $\mathrm{ord}_m b \mid n \wedge \mathrm{ord}_m b \mid 2l \Rightarrow \mathrm{ord}_m b$ odd $\Rightarrow \mathrm{ord}_m b \mid l \Rightarrow b^l \equiv 1 \bmod m$ ∎

MT2P2: 1) Show if p odd prime, $2(p-3)! \equiv -1 \bmod p$: Wilson $\Rightarrow (p-1)! \equiv -1 \bmod p \Rightarrow (p-3)!\underbrace{(p-2)}_{-2}\underbrace{(p-1)}_{-1} \equiv -1 \bmod p \Rightarrow 2(p-3)! \equiv -1 \bmod p$. ∎

2) Compute $3^{3^{4736}} \bmod 23$: FLT $\rightarrow 3^{22} \equiv 1 \bmod 23$. Want $3^{4736} \bmod 22$, $(3, 22) = 1$, $\varphi(22) = \varphi(2)\varphi(11) = 10 \overset{\text{Euler}}{\Rightarrow} 3^{10} \equiv 1 \bmod 22 \Rightarrow 3^{4736} \equiv 3^6 \bmod 22$

Now $3^3 = 27 \equiv 5 \bmod 22 \Rightarrow 3^6 \equiv 25 \bmod 22 \equiv 3 \bmod 22 \Rightarrow 3^{4736} \equiv 3 \bmod 22 \Rightarrow 3^{3^{4736}} \equiv 3^3 \bmod 23 \equiv 4 \bmod 23$ **3)** Let $m, n \in \mathbb{Z}$, $(m,n) = 1$, $(a, mn) = 1$. Suppose $\mathrm{ord}_m(a) = h_1$, $\mathrm{ord}_n(a) = h_2$. Show $\mathrm{ord}_{mn}(a) = \mathrm{lcm}(h_1, h_2) =: l$: $h_1, h_2 \mid l$. $\Rightarrow a^l \equiv 1 \bmod m \equiv 1 \bmod n$. $(m,n) = 1 \Rightarrow a^l \equiv 1 \bmod mn$

Suppose $k < l$ s.t. $a^k \equiv 1 \bmod mn$. By Theorem A: $\Leftrightarrow \begin{cases} a^k \equiv 1 \bmod m \\ a^k \equiv 1 \bmod n \end{cases} \Rightarrow \begin{matrix} h_1 \mid k \\ h_2 \mid k \end{matrix} \Rightarrow l \mid k$. ∎

4) Let $f(x) = x^3 + 8x^2 - x - 1$. Find all solutions to $f(x) \equiv 0 \bmod 11^2$. What about mod 11^n, $n \ge 3$? Note $x \equiv 4, 5 \bmod 11$ roots. mod 11^2: 4 lifts to unique root $4 + 11 \cdot t \pmod{11^2}$. $t \cdot f'(4) \equiv -\frac{f(4)}{11} \bmod 11 \Rightarrow t = \frac{-187}{11} \equiv 5 \bmod 11$. 5 is singular, $f(5) \not\equiv 0 \bmod 121$, doesn't lift to root. $\Rightarrow$ 1 root $\forall n \ge 2$.

5) a) Let $n \in \mathbb{Z}$, $n > 2$. Show $(n, \varphi(n)) = 1 \Rightarrow n$ odd squarefree: $\varphi(n)$ even $\Rightarrow n$ odd. If p odd prime, $p^2 \mid n \Rightarrow p \mid \varphi(n) \wedge p \mid n \Rightarrow (n, \varphi(n)) \ge p$. ∎

b) Show if $m, n \in \mathbb{Z}^+$, $m \mid n \Rightarrow \varphi(m) \mid \varphi(n)$: Decompose into prime factorization. ∎

FEP1: 1) a) T/F: g prim root mod 11 $\Rightarrow g$ prim root 22 : F: 2 is primitive root mod 11 ($\varphi(11) = 10 \wedge 2^1, 2^2, 2^5 \not\equiv 1 \bmod 11$) but $(2, 22) \ne 1$

b) Let p be an odd prime, a, b prim roots mod p. Show ab is not: $b \equiv a^i \bmod p$ for some i, $(i, p-1) = 1$. In particular, i odd since $\mathrm{ord}_p b = \mathrm{ord}_p a = p - 1$. $\Rightarrow ab = a \cdot a^i \equiv a^{i+1} \bmod p$, $i+1$ even $\Rightarrow \mathrm{ord}_p(ab) = \mathrm{ord}_p(a^{i+1}) = \frac{p-1}{(i+1, p-1)} < p - 1$ since $(i+1, p-1) \ge 2$. $\Rightarrow ab$ not prim root

2) Compute $\overbrace{\sum_{d \mid n} \mu(d)\varphi(d)}^{g(n)}$: Since μ, φ multiplicative, so is $\mu \cdot \varphi \Rightarrow$ so is $g(n)$. $\Rightarrow g(p^a) = \sum_{d \mid p^a} \mu(d)\varphi(d) = \underbrace{\mu(1)\varphi(1)}_{1 \cdot 1} + \underbrace{\mu(p)\varphi(p)}_{(-1)(p-1)} + \underbrace{\cdots \mu(p^a)\varphi(p^a)}_{} = 2 - p$

Thus $g(n) = \prod_{p \mid n,\, p \text{ prime}} (2 - p)$. **3)** For what n is $\varphi(n) = \frac{n}{3}$? Let $n = p_1^{a_1} \cdots p_r^{a_r}$, $a_i \ge 1$. Then $\varphi(n) = p_1^{a_1 - 1}(p_1 - 1) \cdots p_r^{a_r - 1} - \frac{1}{3}(p_1^{a_1} \cdots p_r^{a_r}) = 0 \Leftrightarrow 3(p_1 - 1) \cdots (p_r - 1)$

If $p_1, \dots, p_r$ ordered, $p_2, \dots, p_r$ odd, impossible if $r > 2$. Thus $r = 1$ or 2. 1) $r = 1$ $3(p_1 - 1) = p_1$ impossible, $p_1 \mid 3(p_1 - 1) \Rightarrow p_1 = 3$, but this no good. $= p_1 \cdots p_r$

2) $r = 2$ $3(p_1 - 1)\underset{\text{even}}{(p_2 - 1)} = p_1 \underset{\text{odd}}{p_2} \Rightarrow p_1 = 2 \Rightarrow 3(p_2 - 1) = 2p_2 \Rightarrow 3 \mid p_2 \Rightarrow p_2 = 3$. Thus, $n = 2^a \cdot 3^b$, $a, b > 0$. **4)** Find all residues a mod 11 such that $x^n \equiv a \bmod 11$ solvable $\Leftrightarrow a^{\varphi(11)/d} \equiv 1 \bmod 11$ w/ $d = (n, \varphi(11))$ a) a is a square mod 11 : a s.t. $a^{10/2} \equiv 1 \bmod 11 \Leftrightarrow a^5 \equiv 1 \bmod 11$

certainly $a = 1$ is a solution, 2 primitive root 11 $\rightarrow$ other solutions to $a^5 \equiv 1 \bmod 11$ are of the form 2^j with $\mathrm{ord}(2^j) = \frac{10}{(j, 10)} = 5 \Rightarrow (j, 10) = 2 \Rightarrow j$ even

$a \equiv 2^2, 2^4, 2^6, 2^8, 1 \bmod 11 \equiv 4, 5, 9, 3, 1 \bmod 11$ b) cubes mod 11: a's s.t. $a^{10} \equiv 1 \bmod 11$, $d = (3, \varphi(11)) = (3, 10) = 1$. FLT $\Rightarrow$ any $(a, n) = 1$ satisfies the above relation, so they are all cubes mod 11. c) fifth powers mod 11 : a's such that $a^{10/5} \equiv 1 \bmod 11$ $a^2 \equiv 1 \bmod 11 \Rightarrow a \pm 1 \bmod 11$

5) Find all primitive roots mod 125: Can easily check 2 is a primitive root mod 5 $\Rightarrow$ 2 or $2 + 5 = 7$ (or both) is a primitive root mod 5.

Test whether 2 is primitive root mod 25. $\varphi(25) = 20$; $\mathrm{ord}_{25} 2 \mid \varphi(25) = 20 \Rightarrow \mathrm{ord}_{25} 2 = 1, 2, 4, 5, 10, 20$. But $2^1, 2^2, 2^4, 2^5, 2^{10} \not\equiv 1 \bmod 25 \Rightarrow$ 2 prim root mod 25. We know from class that 2 remains prim root mod 125. Any other primitive root must be of the form 2^k, $(k, \varphi(125)) = 1$, $(k, 100) = 1$ $\rightarrow$ there are $\varphi(100) = 40$ such integers. **6)** Show that $N = 4 \cdot 14^k + 1$ is composite $\forall k \ge 1$. Let $N = 4 \cdot 14^k + 1$, c1 k odd, $k = 2n - 1$: $4 \equiv 1 \bmod 3$, $14 \equiv 2 \bmod 3$, $N \equiv 2^{2n+1} + 1 \equiv 4^n \cdot 2 + 1 \equiv 2 + 1 \bmod 3 = 0$ c2 $k = 2n$: $4 \equiv -1 \bmod 5$, $14 \equiv -1 \bmod 5 \rightarrow N \equiv (-1)(-1)^{2n} + 1 \equiv 0 \bmod 5$

7) a) Show 3 prim mod 17 : $\varphi(17) = 16$, $\mathrm{ord}_{17} 3 \mid \varphi(17) = 16 \Rightarrow \mathrm{ord}\, 3 = 1, 2, 4, 8,$ or 16. $3^1, 3^2, 3^4, 3^8 \not\equiv 1 \bmod 17$ b) Solve $7^x \equiv 4 \bmod 17$:

$7^x \equiv 4 \bmod 17 \Leftrightarrow 3^{x \cdot \mathrm{ind}_3 7} = 3^{\mathrm{ind}_3 4} \bmod 17 \Leftrightarrow x \cdot \underbrace{\mathrm{ind}_3 7}_{} \equiv \underbrace{\mathrm{ind}_3 4}_{} \pmod{16} \Rightarrow 11x \equiv 12 \bmod 16 \Leftrightarrow x \equiv 4 \bmod 16$

$3^{11} \equiv 7 \bmod 17$ $3^{12} \equiv 4 \bmod 17$

8) Find # of solutions $x^2 \equiv 4 \bmod m$, m odd

$x^2 \equiv 4 \bmod p^a$ (odd prime) has 2 sols : $\pm 2 \bmod p$. (Lagrange). Let $f(x) = x^2 - 4$, $f'(x) = 2x$, $f'(\pm 2) = \pm 4 \not\equiv 0 \bmod p$ $\Rightarrow$ 2 sols mod p^a (Hensel). If $m = \prod p_i^{a_i}$ odd, $N(m) = \prod N(p_i^{a_i}) = 2^r$ is # of sols.

FEP2 1) # sols of $x^4 \equiv 61 \bmod 117$. $117 = 3^2 \cdot 13$. $x^4 \equiv 61 \equiv 1 \bmod 3$ has 2 sols: 1, 2. $f'(1), f'(2) \not\equiv 0 \bmod 9$, $\rightarrow$ 2 sols mod 9.

Now consider mod 13. $d = (4, \varphi(13)) = (4, 12) = 4$. Solvable $\Leftrightarrow 9^{\varphi(13)/4} = 9^{12/4 = 3} \equiv 1 \bmod 13 \Rightarrow d = 4$ sols mod 13. $N(117) = N(9)N(13) = 8$. (mult.)

2) Compute $\sum_{d \mid n} \mu(d)^2 \varphi(d)^2$: Consider $F(n) = \sum_{d \mid n} \mu(d)^2 \varphi(d)^2$. Note $F(n)$ multiplicative ($f(n) = \mu(n)^2 \varphi(n)^2$). Let p be prime. Then

$F(p^n) = \sum_{d \mid p^n} \mu(d)^2 \varphi(d)^2 = 1 + (p-1)^2$. Thus $F(n) = \prod_{p \mid n \text{ prime}} [1 + (p-1)^2]$ **3)** Solve $\begin{cases} 9x \equiv 3 \bmod 15 \\ 5x \equiv 7 \bmod 21 \\ 7x \equiv 4 \bmod 13 \end{cases}$ $\begin{matrix} \longleftrightarrow \begin{cases} 0 \equiv 0 \bmod 3 \\ x \equiv 2 \bmod 5 \end{cases} \\ \longleftrightarrow \begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 0 \bmod 7 \end{cases} \\ \longrightarrow x \equiv 8 \bmod 13 \end{matrix}$ $\rightarrow$ CRT

4) Find all sols to $x^2 + 1 \equiv 0 \bmod 65$. $\Leftrightarrow x^2 \equiv -1 \bmod 65 = 5 \cdot 13 \Rightarrow x = 2, 3 \bmod 5$, $5, 8 \bmod 13 \Rightarrow 4$ sols. use CRT.

5) Show $\prod_{d \mid n,\, d > 0} d = n^{\tau(n)/2}$: $\Leftrightarrow \prod d^2 = n^{\tau(n)}$. Since $\{d \mid n\} = \{\frac{n}{d}, d \mid n\}$, $\prod d^2 = (\prod d)(\prod d) = \prod d \prod \frac{n}{d} = \prod n$ ✓

6) Compute $(102^{73} + 55)^{37} \bmod 111$: $111 = 3 \cdot 37$. mod 3: $102^{73} \equiv 0 \bmod 3$ $55 \equiv 1 \bmod 3 \Rightarrow 102^{73} + 55 \equiv 1 \bmod 3$

mod 37: $102 \equiv 28 \bmod 37$, $\varphi(37) = 36$, $73 = 2 \cdot 36 + 1 \rightarrow 102^{73} \equiv 28^{73} = 28^{2 \cdot 36} \cdot 28 \equiv 28 \bmod 37$. $55 \equiv 18 \bmod 37 \Rightarrow$

$102^{73} + 55 \equiv 46 \equiv 9 \bmod 37 \rightarrow (102^{73} + 55)^{37} \equiv 9^{37} \pmod{37} \equiv 9 \bmod 37$. Solve $\begin{cases} A \equiv 1 \bmod 3 \\ A \equiv 9 \bmod 37 \end{cases} \overset{\text{CRT}}{\Rightarrow} A \equiv 46 \bmod 111$.

7) Use Mobius to find $f(n)$: $\sum_{d \mid n} f(d) = \frac{(-1)^n + 1}{2}$ $\forall n \ge 2$. Let $g(n) = \frac{(-1)^n + 1}{2} = \begin{cases} 1 & n \text{ even} \\ 0 & n \text{ odd} \end{cases}$ Since $\sum_{d \mid n} f(d) = g(n)$, Mobius $\Rightarrow$

$f(n) = \sum_{d \mid n} \mu(\frac{n}{d}) g(d) = \sum_{d \mid n \text{ even}} \mu(\frac{n}{d}) = \sum_{2k \mid n} \mu(\frac{n}{2k}) = \sum_{k \mid \frac{n}{2}} \mu(\frac{n/2}{k}) = \begin{cases} 1 & n/2 = 1 \\ 0 & \end{cases} \Rightarrow f(n) = \begin{cases} 1 & n = 2 \\ 0 & \end{cases}$