1. $6^x \equiv A \mod 37$ can have how many solutions mod 36 for different values of A?

Soln: if $A \equiv 0 \mod 37 \Rightarrow$ no solns

order of 6 mod 37:

$6^2 \equiv 36 \equiv -1 \mod 37$

$\Rightarrow 6^4 \equiv 1 \mod 37$

$\Rightarrow \text{ord}(6) \mid 4 \Rightarrow \text{ord}(6) = 4$

$6^x \equiv A$ has solns iff $A \equiv 6^B$ for some B

$6^x \equiv 6^b \mod 36$

$\iff x \equiv b \mod \text{ord}(6) = 4$

$\Rightarrow$ unique soln for $x \mod 4$

$\Rightarrow 36/4$ solns mod 36

" 9 solns mod 36

2. $x^{14} \equiv A \mod 37$, $A \not\equiv 0$ has how many solns?

0, 2

Soln: Let g be a primitive root mod 37.

Let $x = g^y$, $A = g^B$

$\Rightarrow g^{14y} \equiv g^b \mod 37$

$\Rightarrow 14y \equiv b \mod \text{ord}(g) = 36$ (*)

$\rightsquigarrow 14y - b = 36k$

$\Leftrightarrow 14y - 36k = b$

$\gcd(14, 36) = 2 \mid \text{LHS}$

no solns if $2 \nmid b$

$\Rightarrow 7y \equiv b/2 \mod 18$

$y = 7^{-1}(b/2)$ unique soln mod 18

$\Rightarrow 36/18 = 2$ solns mod 36

3. T/F, half of the elements $\{1, 2, \ldots, 22\}$ are primitive roots mod 23.

Soln: F

$\#\text{p.r. mod } 23 = \varphi(23-1)$

$= \varphi(22)$

$\varphi(2 \cdot 11) = \varphi(2)\varphi(11)$

$= 1 \cdot 10 < \frac{22}{2} = 11$

4. T/F if g is a p.r. mod p, then g^2 is <u>not</u> a p.r.

Soln: $(g^2)^{\frac{p-1}{2}} = g^{p-1} = 1$

$\Rightarrow \text{ord}(g^2) \leq \frac{p-1}{2} < p-1$

$\Rightarrow g^2$ <u>not</u> a p.r.

T/F

5. Let $p = 4k+1$ be prime

Then # primitive roots mod p is even.

Soln: T

$$\#_{p.r.s} = \varphi(p-1) = \varphi(4k)$$

Let $4k = 2^s \cdot t$, $2 \nmid t$.

$s \geq 2$

$$\varphi(4k) = \varphi(2^s t) = \varphi(2^s)\varphi(t)$$

$$= 2^{s-1}\varphi(t)$$

$s-1 > 0$, so $\uparrow$ is even

$\square$

sq-free

6. Prove that if $x^2 - Dy^2 = M$ (*) has a soln, it has infinitely many solns.

Pf: (**) $x^2 - Dy^2 = 1$ has a soln since D sq-free.

Let (x_1, y_1) solve (**)

• Let $\xi^2 - D\eta^2 = M$

(x_k, y_k), where

$$x_k + y_k\sqrt{D} = (x_1 + y_1\sqrt{D})^k$$

solves (**)

Consider (ξ_k, η_k), where

$$\xi_k + \eta_k = (\xi + \eta\sqrt{D})(x_1 + y_1\sqrt{D})^k$$

$$(\xi+\eta\sqrt{D})(x_1+y_1\sqrt{D})^k(\xi-\eta\sqrt{D})(x_1-y_1\sqrt{D})^k$$

$$=(\xi^2-D\eta^2)(x_1^2-Dy_1^2)^k$$

$$=M\cdot 1^k=M \qquad <1/b^D$$

$\square$

7. Show that $\left|\frac{a}{3^n}-(\sqrt{7}+1)\right|\leq 1/10^n$ has finitely many solns $\forall a,n$.

Pf: Idea: Liouville: if α is a root of $f(x)\in\mathbb{Z}[x]$, degree d

$\Rightarrow \left|\frac{a}{b}-\alpha\right|\leq 1/b^D$ has finitely many solns $\forall D>d$

build a poly w/ roots $1+\sqrt{7}$, $1-\sqrt{7}$

x^2-2x-6 has $\nearrow$ as roots

$\alpha = \frac{1+\sqrt{7}}{2}$

$\Rightarrow \alpha$ is degree 2, $d=2$

$\Rightarrow \left|\frac{a}{b} - \alpha\right| \leq \frac{1}{b^D}$ has finitely many solns $\forall D > 2$.

$b = 3^n$

$\left|\frac{a}{b} - \alpha\right| \leq \frac{1}{10^n}$

$\varepsilon > 0$

$10^n = \left(3^{2+\varepsilon}\right)^n = \left(b^{2+\varepsilon}\right)$

$\Rightarrow \frac{1}{10^n} \leq \frac{1}{(3^2)^n}$

if $b = 3^n$, then

$\left|\frac{a}{b} - \alpha\right| < \frac{1}{10^n} = \frac{1}{(3^{2+\varepsilon})^n} = \frac{1}{b^{2+\varepsilon}}$

only finitely many solns