Q) Prove that any number of the form 2^k looks like $100\cdots0$ in base 2

Ans:- $(a_n a_{n-1} \cdots a_1 a_0)_2 < 2^{n+1}$

Base Case:- $1 < 2^1$, $0 < 2^1$ $\quad 10 = 2^1$

Induction Assumption:- $(1\underbrace{00\cdots0}_{n})_2 = 2^{n+1}$

Inductive Step:- $(1\underbrace{00\cdots0}_{n+1})_2 = 1\times 2^{n+2} + 0\times 2^{n+1} - - - - 0\times 2^0)$
$= 2(1\times 2^{n+1} + 0\times 2^n + \cdots + 0\times 2^0)$
$= 2\; 2^{n+1} = 2^{n+2}$

Theorem in ONT:- For natural numbers a, m, n, we have $\gcd(a^m-1, a^n-1) = a^{\gcd(m,n)} - 1$

Ans:- Hint is in ONT book page 12.
Do the full proof (HomeWork)

there exists
$\exists\, x, y$ such that,
$mx + ny = \gcd(m,n)$

WLOG let $m \geq n$
$\gcd(a^m-1, a^n-1)$
$= \gcd(a^m - 1 - a^{m-n}(a^n-1), a^n-1)$
$= \gcd(a^m - 1 - a^m - a^{m-n}, a^n-1) = \gcd(a^{m-n}-1, a^n-1)$

Doing this $\lfloor \frac{m}{n} \rfloor$ times we get $\gcd(a^m-1, a^n-1) = \gcd(a^r-1, a^n-1)$

Now $r < n$, so we can use Euclid's algorithm in the powers of a.

$\gcd(a^r-1, a^n-1)$
$= \gcd(a^{n-r}-1, a^r-1) \cdots\cdots = \gcd(a^{r_n}-1, a^{r_{n-1}}-1) \cdots = \gcd(a^0-1, a^{r_n}-1)$
$= \gcd(0, a^{r_n}-1)$
$= a^{r_n} - 1 = a^{\gcd(m,n)} - 1$

Q) Show that $\sqrt{2}$ is an irrational number

Ration Numbers + Irrational Numbers
||
Real Numbers

Ans:- Suppose $\sqrt{2}$ is rational number
$\Rightarrow \sqrt{2} = \frac{m}{n}$ where $\gcd(m,n) = 1$ & $m, n \in \mathbb{Z}$, $n \neq 0$

$m = 2^{\alpha_1} p_1 p_2 p_3 \cdots$
$m^2 = 2^{2\alpha_1}$

$\frac{m^2}{n^2} = 2 \Rightarrow m^2 = 2n^2 \Rightarrow 2 \mid m^2 \Rightarrow 2 \mid m$
$\Rightarrow 4 \mid m^2$

$4 \mid 2n^2$
$\Rightarrow 2 \mid n^2 \Rightarrow 2 \mid n \Rightarrow \gcd(m,n) = 1$

contradiction

$\Rightarrow \sqrt{2}$ is irrational

Q) Prove that $\sqrt{p}$ is irrational for prime p.

Ans:- Suppose $p = \frac{m}{n}$ (m, n) are coprime

$\sqrt{p} = \frac{m^2}{n^2} \Rightarrow p\, n^2 = m^2 \Rightarrow p \mid m^2 \Rightarrow p \mid m$ as p is prime

$\Rightarrow p^2 \mid m^2$

$p^2 \mid p n^2 \Rightarrow p \mid n^2 \Rightarrow p \mid n \Rightarrow \gcd(m, n) \neq 1$

contradiction

$\Rightarrow \sqrt{p}$ is irrational

Q) If p is prime and $0 < k < p$ prove that $\binom{p}{k}$ is divisible by p.

Ans:- $\binom{p}{k} = \frac{p!}{k!\,(p-k)!} = \frac{p\,(p-1) \cdots 1}{k!\,(p-k)} = p\left(\frac{(p-1)!}{k!\,(p-k)!}\right) \in \mathbb{Z}$

$= pM$

If M is not an integer then, $M = \frac{N}{p}$ where $N \in \mathbb{Z}$

M consist of numbers from 1 to $p-1$, in the form $\frac{(p-1)!}{k!\,(p-k)!}$ and as p is prime it is not divisible by any number except 1 and p.

$\Rightarrow p \nmid M$ but $pM \in \mathbb{Z} \Rightarrow M \in \mathbb{Z}$

$\Rightarrow p \mid \binom{p}{k}$

Four Number Lemma:-

Let a, b, c, d be positive integers such that $ab = cd$. Show that there exists positive integers p, q, r, s such that

$\frac{a}{c} = \frac{d}{b}$

$a = pq, \quad b = rs, \quad c = ps, \quad d = qr$

Proof:- We have $\frac{a}{c} = \frac{d}{b} = \frac{q}{s}$ $\qquad \gcd(q, s) = 1$

$a = \frac{cq}{s} = pq$ then $\qquad d = \frac{bq}{s} = qr$ then

$a = \frac{cq}{s} = pq$ ← then take $\frac{c}{s} = p \Rightarrow c = ps$

$d = \frac{bq}{s} = qr$ ← then take $\frac{b}{s} = r \Rightarrow b = rs$

Q) Prove that if $ab = cd$ (a, b, c, d are positive integers), then $a+b+c+d$ is not prime

Ans:- $a+b+c+d = pq + qr + ps + qr$

$= r(q+s) + p(q+s) = (p+r)(q+s) \Rightarrow$ not prime

'cas $p+r,\ q+s \geq 2$

Q) ARMO 1995 (→ All Russia Mathematics Olympiad) :- Let m, n be positive integers such that,

$$\gcd(m,n) + \operatorname{lcm}(m,n) = m+n$$

Show that one of the two numbers is divisible by other

Ans:- $\gcd(m,n) = d$ $\quad m = dk_1,\ n = dk_2$

$\operatorname{lcm}(m,n) = dk_1k_2$

$d + dk_1k_2 = dk_1 + dk_2$

$\Rightarrow 1 + k_1k_2 = k_1 + k_2$

$\Rightarrow k_1k_2 - k_2 = k_1 - 1 \Rightarrow k_2(k_1 - 1) = k_1 - 1$

If $k_1 > 1 \Rightarrow k_2 = 1 \Rightarrow n = d \Rightarrow n \mid m$

If $k_1 = 1 \Rightarrow m = d \Rightarrow m \mid n$

Q) If p is an odd prime and a, b are coprime then show that,

$$\gcd\left(\frac{a^p + b^p}{a+b},\ a+b\right) \in \{1, p\}$$

Ans - Hint:- Factorize it first, then again factorize with leaving a remainder (Home Work)

Q) Show that any composite number n has a prime factor $\leq \sqrt{n}$

$\qquad \alpha_1 \qquad\qquad \alpha_k$

Q> Show that any composite

Ans:— $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

Suppose p_i's are all $> \sqrt{n}$

$\Rightarrow p_1 p_2 > n$ not possible $\Rightarrow \exists\, p_i$ such that $p_i \leq \sqrt{n}$

two primes will be as n is composite