Sample Questions from Number Theory

State the Division Algorithm.

State the well ordering (W.O.) principle.

Define $\gcd(a,b)$.

State the Fundamental Theorem of Arithmetic.

Let $a, b \in \mathbb{Z}$, $b > 0$. Use W.O. to prove the existence of integers q, r so that $a = bq + r$, $0 \le r < b$.

Let $a, b \in \mathbb{Z}^+$. Use W.O. to prove that (~~the least etc.~~) $\gcd(a,b)$ can be written as $\gcd(a,b) = sa + tb$ for some $s, t \in \mathbb{Z}$.

Define $a \mid b$.

Prove that if $\gcd(a,b) = 1$ and $a \mid bc$, then $a \mid c$.

Use Euclidean Algorithm to find $\gcd(36, 64)$ and to find integers s, t so that $\gcd(36, 64) = s(36) + t(64)$.

Use Fund Th^m to prove that $\sqrt[3]{6} \notin \mathbb{Q}$.

Use Fund Th^m to prove that the only integers whose square roots are rational are the perfect squares. (same for cubes & cube roots).

Use Fund Th^m to prove that $\log_2(10) \notin \mathbb{Q}$.

If $\frac{a^2}{b^2} = 2$, then show that $\frac{2b - a}{a - b} = \frac{a}{b}$. Use this fact and W.O. to prove that $\sqrt{2} \notin \mathbb{Q}$.

Prove that there are primes $> n$ for every $\oplus$ integer n as follows: consider $n! + 1$.

Prove that $\gcd(a, a+1) = 1$ for any $a \in \mathbb{Z}^+$.

Prove that $\gcd(a, a+2) = 1$ or 2 for $a \in \mathbb{Z}^+$
(when do you get 1, when 2).

Suppose that $\gcd(a, b) = 1$. Prove that $\gcd(a+b, a-b) = 1$ or 2.

Suppose $k \in \mathbb{Z}^+$. Show that $6k-1$, $6k+1$, $6k+2$, $6k+3$, $6k+5$ are all pairwise relatively prime.

Let $a, b, c \in \mathbb{Z}^+$. Show that $\gcd(a, b, c)$ can be expressed as a combination $sa + tb + uc$ for some $s, t, u \in \mathbb{Z}$.

Use Euc Algorithm to compute $\gcd(102, 222)$ $\gcd(20785, 44350)$ $\gcd(51, 87)$ $\gcd(981, 1234)$.	Write out prime factorization of $10!$ $20!$ How many zeros at end of $1000!$?