1. Prove that if $b$ has an inverse in $\mathbb{Z}_n$, then it is unique.

2. (a) Compute $2^{38} \mod 7$.
(b) Compute $3^{29} \mod 20$.
(c) Compute $5^{33} \mod 13$.

3. (a) Show that $a^k - 1$ is a multiple of $a - 1$ for any positive $a$ and $k$.
(b) Show that if positive $m$ and $n$ are not relatively prime, then $2^m - 1$ and $2^n - 1$ are not relatively prime.
(c) Show that if positive $m$ and $n$ are relatively prime, then $2^m - 1$ and $2^n - 1$ are relatively prime.

4. Consider the following game. Some number $n$ is chosen, and on a piece of paper is written down all its factors (including itself and 1). The two players take turns naming a factor that has not been crossed out. Each time they name a factor, that factor and all multiples of it are crossed out. The player who has to take the factor 1 loses.

For example, suppose $n = 24$. The factors are 1, 2, 3, 4, 6, 8, 12, and 24. Say the first player names 4. Then the remaining factors are 1, 2, 3, and 6. Say the second player names 3. Then, the remaining factors are 1 and 2. The first player clearly names the 2, and the second player loses.

(a) Show that the first player can always win if $n$ is prime or a power of a prime.
(b) Show that the first player can always win if $n$ is a product of two distinct primes.
(c) What should happen for $n = 24$ if both players play optimally?

Due: 10:10am Wednesday 6 October