Winter Math Camp: Number Theory

Dan Brown, Certicom Research

January 9, 2004, Toronto

1. Let $n, x \in \mathbb{Z}$, with $n > \overset{2}{\cancel{1}}$. Show $x^2 \not\equiv \overset{5}{\cancel{3}} \bmod 2^n$.
2. Let $f_p(x) = \frac{x^{p-1}-1}{p}$. If $a, p \in \mathbb{Z}$ with p prime, show $f_p(a) \in \mathbb{Z}$.
3. With a, p, f_p as above, and $b \in \mathbb{Z}$, $p \nmid ab$, show $f_p(ab) \equiv f_p(a) + f_p(b) \bmod p$.
4. With p and f_p as above, is it true that $f_p(g^y \bmod p) \equiv y f_p(g) \bmod p$? Why, or why not?
5. Let $a, b \in \mathbb{Z}$. If $a, b \geq 0$ and $c = \frac{a^2+b^2}{1+ab} \in \mathbb{Z}$, show $\sqrt{c} \in \mathbb{Z}$.
6. If $n \in \mathbb{Z}$ has prime factorization $n = p^r q^s$, what's the chance $x^n \equiv y \bmod n$ has an integer solution x given random $y \in \mathbb{Z}$?
7. Let p be a prime, and let $d_{i,j}$ be integers in $[0, p-1]$. Let $n_i = \sum_{j \geq 0} d_{i,j} p^j$. Show $\binom{n_1+n_2}{n_1} \equiv \prod_{j \geq 0} \binom{d_{1,j}+d_{2,j}}{d_{1,j}} \bmod p$.
8. Let p_i be the i^{th} prime, and let $w(p_{i_1} p_{i_2} \cdots p_{i_s}) = 1 + w(i_1) + \cdots + w(i_s)$. For each $n \geq 1$, find maximal and minimal solutions to $w(z) = n$.
9. For each n, find $P_1, \ldots, P_n \in \mathbb{R}^2$ with $P_i P_j P_k$ non-collinear and $|P_i P_j| \in \mathbb{Z}$ for all i, j, k.
10. Let $C_0 = 2$. Let $C_{n+1} = 2^{C_n} - 1$. Show $C_n | 2^{C_n - 1} - 1$ for all n.
11. With C_n as above, show that if C_{n+1} is prime then $2C_n+1$ is composite.
12. Let p be prime, and let $1 < t < p$. Let $q = tp + 1$. Suppose $a^p \equiv 1 \bmod q$ and $\gcd(a-1, q) = 1$. Show q is prime.
13. What's the least number k with every number being the sum of k triangular numbers ($T_m = m(m+1)/2$, $m \geq 0$)?
14. ~~Is~~ 2004 ~~ever~~ is the least value of m with $\gcd(a, n) = 1 \Rightarrow a^m \equiv 1 \bmod n$?

Does $\exists$ n st