Some number theory

October 3, 2008

Throughout, p denotes a prime, n denotes a positive integer, a denotes a number coprime to n (or p), and $\phi(n)$ denotes the number of positive integers between 1 and n (inclusive) that are coprime to n. We have

- **Fermat's theorem** $a^{p-1} \equiv 1 \pmod{p}$
- **Euler's theorem** $a^{\phi(n)} \equiv 1 \pmod{n}$
- **Wilson's theorem** $(p-1)! \equiv -1 \pmod{p}$

Slightly deeper is the fact that

- **Every prime has a primitive root**

What this means is: take any prime number, for instance 7. It is possible to generate all the numbers $1, 2, 3, 4, 5, 6$ as successive powers of one of them. In this case either 3 or 5 will do. So $3^1 = 3 \equiv 3, 3^2 = 9 \equiv 2, 3^3 = 27 \equiv 6, 3^4 = 81 \equiv 4, 3^5 = 243 \equiv 5$ and $3^6 = 729 \equiv 1$, all modulo 7. (This does not work with $2, 4, 6$ or 1.) 3 is called a **primitive root** mod 7. Exercise: find a primitive root mod 11.

It is easy to prove both Fermat's and Wilson's theorems using this fact (exercise). Also, the **quadratic residues** are just the even powers of a primitive root.

Examples

1. (Balkan Olympiad) Show that the equation $x^3 + y^4 = 7$ has no integer solutions x, y.

2. (Putnam 1985) Define a sequence $\{a_i\}$ by $a_1 = 3$ and $a_{i+1} = 3^{a_i}$ for $i \geq 1$. Which integers between 00 and 99 inclusive occur as the last two digits in the decimal expansion of infinitely many a_i?

Homework

1. (Putnam 1954) Prove that there are no integers x and y for which $x^2 + 3xy - 2y^2 = 122$. [**Hint.** Try completing the square on the left hand side.]
2. (Putnam 1997, paraphrased) Define a sequence $\{a_i\}$ by $a_1 = 2$ and $a_{i+1} = 2^{a_i}$ for $i \geq 1$. Prove that $a_n \equiv a_{n-1} \pmod{n}$ for $n \geq 2$.