Lecture 13: Congruences — Math 345

Wednesday, October 13, 2010 — Jim Fowler

Textbook

This lecture discusses section 4 of the textbook.

Homework

The homework is due Wednesday, October 20, 2010.

From Section 4 of the textbook, do exercises 25 and 26.

equivalence relations

well-defined

hardy and the usefulness of number theory

Hardy said: “I have never done anything ‘useful’. No discovery of mine has made, or is likely to make, directly or indirectly, for good or ill, the least difference to the amenity of the world.”

This turns out to be false.

Number theory is incredibly important to internet commerce.

prime numbers are important.

factoring numbers is hard.

simple example: proving that I wrote a secret document. include the product of two large primes. at a future date, i declare “the huge number on the secret document is the product of p and q” which proves that I must have written the document.

public-key cryptosystems

341 is pseudoprime

modulo 11

$341 = 31 \times 11$.

$$2^{11} \equiv 2 \pmod{11}$$

$$2^{31} \equiv 2^{11} \cdot 2^{11} \cdot 2^{9} \equiv 2^{11} \equiv 2 \pmod{11}.$$

$$2^{341} \equiv \left(2^{31}\right)^{11} \equiv 2^{11} \equiv 2 \pmod{11}.$$

modulo 31

$$2^{31} \equiv 2 \pmod{31}$$

$$2^{341} \equiv 2^{11} \pmod{31}$$

$$2^{11} \equiv 2^{5} \cdot 2^{5} \cdot 2 \equiv (-1) \cdot (-1) \cdot 2 \equiv 2 \pmod{31}$$

combining these facts (without yet knowing CRT)

$2^{341} \equiv 2 \pmod{11}$ and $2^{341} \equiv 2 \pmod{31}$.

since $2^{341} = 2 + 31k$ possible residues mod 341: 2, 33, 64, 95, 126, 157, 188, 219, 250, 281, 312

since $2^{341} = 2 + 11k$ possible residues mod 341: 2, 13, 24, 35, 46, 57, 68, 79, 90, 101, 112, 123, 134, 145, 156, 167, 178, 189, 200, 211, 222, 233, 244, 255, 266, 277, 288, 299, 310, 321, 332

necklace proof of fermat's little theorem

one of many proofs

this is the easiest to see, i think.

find last digit

Find the last digit of 2^{1000}.

$2^{1000} \equiv (2^5)^{200} \equiv 2^{200} \equiv 2^{40} \equiv 2^8 \equiv 1 \pmod 5$
$2^{1000} \equiv 0 \pmod 2$
so $2^{1000} \equiv 6 \pmod{10}$

solving linear equations?

solving quadratic equations?

what about square roots modulo n?

example from hensel's lemma

find a number x so that . . .

$x^2 \equiv 2 \pmod 7$. say $x = 3$
$x^2 \equiv 2 \pmod{49}$. say $x = 3 + 7k$, say, $x = 10$.
$x^2 \equiv 2 \pmod{343}$. say $x = 10 + 49k$, say, $x = 108$.
$x^2 \equiv 2 \pmod{2401}$. say $x = 108 + 343k$, say, $x = 794$.

better example

find a number x so that

$x^3 \equiv 7 \pmod{10}$. say $x = 3$.
$x^3 \equiv 7 \pmod{100}$. say $x = 3 + 10k = 43$.
$x^3 \equiv 7 \pmod{1000}$. say $x = 43 + 100k = 543$.
$x^3 \equiv 7 \pmod{10000}$. say $x = 43 + 100k = 543$.

best example

find a number x so that

$x^2 \equiv 3 \pmod{11}$. say $x = 6$.
$x^2 \equiv 3 \pmod{121}$. say $x = 6 + 11k = 6 + 11 \cdot 8 = 94$.
$x^2 \equiv 3 \pmod{1331}$. say $x = 94 + 121k = 94 + 121 \cdot 4 = 578$.
$x^2 \equiv 3 \pmod{14641}$. say $x = 578 + 1331k = 578 + 1331 \cdot 2 = 3240$.