# Math 126 Number Theory

Prof. D. Joyce, Clark University

10 Feb 2006

**Due Today.** From page 43, exercises 2, 3, 5, 6, 7.

**Due Wednesday.** From page 47, exercises 3–8, 10, 12.

**Due next Friday.** From page 54: 1–5, 8, 10; and from page 63: 1, 4–6, 8, 9, 13, 19–21.

**First test.** Wednesday, Feb. 22.

**For next time.** We'll begin section 3.3 on linear congruence equations.

**Last meeting.** Linear Diophantine equations.

**Today.** Congruence modulo $n$. When a number $n$ divides the difference $a - b$ of two other numbers $a$ and $b$, we say that $a$ is *congruent* to $b$ *modulo* $n$, denoted

$$a \equiv b \pmod{n}.$$

When $n$ doesn't divide the difference $a - b$, we say $a$ is not congruent to $b$, denoted $a \not\equiv b \pmod{n}$.

You're familiar with congruence modulo 12; it's what 12-hour clocks use.

We may discuss the "mind reading" game in the text. The trick in that game comes down to a particular equation modulo 1000, namely

$$143 \cdot 7 \equiv 1 \pmod{1000}.$$

**Properties of congruence.** Congruence modulo $n$ has many of the same properties that equality has. First of all, it's an equivalence relation. An *equivalence relation* is a relation that is reflexive, symmetric, and transitive.

Reflexive: $\forall a,\ a \equiv a \pmod{n}$.

Symmetric: $\forall a, \forall b,\ a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$.

Transitive: $\forall a, \forall b, \forall c,\ a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ implies $a \equiv c \pmod{n}$.

We'll prove these properties hold for congruence modulo $n$ as well as some of those mentioned in the next paragraph.

Besides being an equivalence relation, congruence modulo $n$ works well with three of the operations of algebra, namely, addition, subtraction, and multiplication. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$, $a - c \equiv b - d \pmod{n}$, and $ac \equiv bd \pmod{n}$.

But congruence modulo $n$ doesn't work so well with division. Although $49 \equiv 25 \pmod{6}$ and $7 \equiv 1 \pmod{6}$, it is not the case that $49/7 \equiv 10/1 \pmod{6}$.