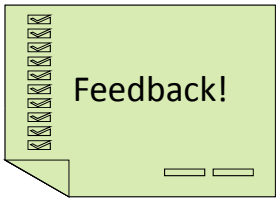
ACM ICPC

- Teams set?
- Seven rooms reserved
- Checking on vans (2); need backup drivers
- Maintain your profile at Baylor site*
- Need to set date/time for practice contest* Remaining..
  - Friday, Oct 16 @ 6pm
  - Monday, Oct 19 @ 6pm
  - Friday, Oct 23 @ 6pm
  - Sunday, Oct 25@ 12pm

*See my homepage or Facebook group for links

Upcoming Schedule



- Oct 6 (today) – Number Theory
- Oct 13 – October break
- Oct 20 – Backtracking
- Oct 27 – Graph Traversal (Zhanibek)
- Nov 3 – Graph Algorithms (Atallah?)
- Nov 10 – Dynamic Programming
- Nov 17 – Grids
- Nov 24 – no class

Today's Topic

- Number theory
- Concepts to know
  - Prime numbers
  - Divisibility
  - Modular arithmetic
  - Congruences

Prime Numbers

- Prime factorizations are unique "fundamental theorem of arithmetic"
- Finding primes by repeated division

Divisibility

- Equivalent, for integers a and b…
  a | b ("a divides b")
  b % a == 0
  a*k == b, for some integer k
- Greatest Common Divisor, gcd
  – Euclid's algorithm
  – a * x + b * y = gcd(a,b)
- Least Common Multiple, lcm
  lcm(x, y) = x*y/gcd(x, y)

Modular Arithmetic

- Allows some computations without bignums
- Useful identities
  (x + y) % n == ((x % n) + (y % n)) % n
  (x – y) % n == ((x % n) – (y % n)) % n
  -x % n == (n-x) % n
  (x * y) % n == ((x % n) * (y % n)) % n
- Example: Finding the last digit of 2^{100}

Congruences

- Alternative notation for modular arithmetic
- Equivalent, for integers a, b, and n

  $a \equiv b \pmod{n}$

  a % n == b

  n | (a – b)
- Addition, subtraction, multiplication "work" preserving modulus
- Division: OK to divide out common factors of all three numbers, a, b, and n

Solving Linear Congruences

- Given integers a, b, and n, solve

  $ax \equiv b \pmod{n}$

  for x.

Other Hints

- Java: No unsigned, watch for long vs int
- BigInteger in Java includes
  - gcd
  - modPow
  - modInverse
  - isProbablePrime
- UNIX is your friend
  - factor command
  - bc arbitrary precision calculator

Today's Problems

- 110701 Light, More Light
- 110702 Carmichael Numbers
  - "Presentation Error" bug (?) on PC site
- 110703 Euclid Problem
  - Use "extended Euclid algorithm", e.g., from text
- 110704 Factovisors

Today's Problems -- Hints

- 110701 Light, More Light
  - Brute force or counting divisors = timeout
  - Need trick: no loops (!)
- 110702 Carmichael Numbers
  - BigInteger works, but not needed (try without)
- 110703 Euclid Problem
  - Use "extended Euclid algorithm", e.g., from text
- 110704 Factovisors
  - Factor m; count primes in n!