Massachusetts Institute of Technology
6.042J/18.062J, Spring '15: Mathematics for Computer Science March 6
Prof. Albert R Meyer & Prof. Adam Chlipala revised Wednesday 25th February, 2015, 17:59

In-Class Problems Week 5, Fri.

Problem 1.

(a) Use the Pulverizer to find integers x, y such that

$$x30 + y22 = \gcd(30, 22).$$

(b) Now find integers x', y' with $0 \leq y' < 30$ such that

$$x'30 + y'22 = \gcd(30, 22)$$

Problem 2. (a) Let $m = 2^9 5^{24} 11^7 17^{12}$ and $n = 2^3 7^{22} 11^{211} 13^1 17^9 19^2$. What is the $\gcd(m, n)$? What is the *least common multiple*, $\text{lcm}(m, n)$, of m and n? Verify that

$$\gcd(m, n) \cdot \text{lcm}(m, n) = mn. \tag{1}$$

(b) Describe in general how to find the $\gcd(m, n)$ and $\text{lcm}(m, n)$ from the prime factorizations of m and n. Conclude that equation (1) holds for all positive integers m, n.

Problem 3.

The *Binary GCD* state machine computes the GCD of integers $a, b > 0$ using only division by 2 and subtraction, which makes it run very efficiently on hardware that uses binary representation of numbers. In practice, it runs more quickly than the more famous Euclidean algorithm described in Section 8.2.1 in the course textbook.

$$\begin{aligned}
\text{states} &::= \mathbb{N}^3 \\
\text{start state} &::= (a, b, 1) \\
\text{transitions} &::= \text{ if } \min(x, y) > 0, \text{ then } (x, y, e) \longrightarrow
\end{aligned}$$

$$(x/2, y/2, 2e) \qquad (\text{if } 2 \mid x \text{ and } 2 \mid y) \tag{2}$$

$$(x/2, y, e) \qquad (\text{else if } 2 \mid x) \tag{3}$$

$$(x, y/2, e) \qquad (\text{else if } 2 \mid y) \tag{4}$$

$$(x - y, y, e) \qquad (\text{else if } x > y) \tag{5}$$

$$(y - x, x, e) \qquad (\text{else if } y > x) \tag{6}$$

$$(1, 0, ex) \qquad (\text{otherwise } (x = y)). \tag{7}$$

(a) Use the Invariant Principle to prove that if this machine stops, that is, reaches a state (x, y, e) in which no transition is possible, then $e = \gcd(a, b)$.

(b) Prove that rule (2)

$$(x, y, e) \rightarrow (x/2, y/2, 2e)$$

is never executed after any of the other rules is executed.

(c) Prove that the machine reaches a final state in at most $1 + 3(\log a + \log b)$ transitions. (This is a coarse bound; you may be able to get a better one.)

Problem 4.

For nonzero integers, a, b, prove the following properties of divisibility and GCD'S. (You may use the fact that $\gcd(a, b)$ is an integer linear combination of a and b. You may *not* appeal to uniqueness of prime factorization because the properties below are needed to *prove* unique factorization.)

(a) Every common divisor of a and b divides $\gcd(a, b)$.

(b) If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

(c) If $p \mid bc$ for some prime, p, then $p \mid b$ or $p \mid c$.

(d) Let m be the smallest integer linear combination of a and b that is positive. Show that $m = \gcd(a, b)$.

6.042J / 18.062J Mathematics for Computer Science
Spring 2015