More on Number Theoretic Algorithms

CS255

Chris Pollett

Apr. 3, 2006.

Outline

- More Number Theory Definitions
- Euclid’s Algorithm
- Modular Arithmetic

More Number Theory Definitions and Facts

- We say two numbers are **relatively prime** if gcd(a,b) =1.
- We say a list of integers n_1, .., n_k are **pairwise relatively prime** if gcd(n_i, n_j) =1 for i ≠ j.

Theorem (**). If gcd(a, p) = 1 and gcd(b,p) =1, then gcd(ab,p)=1.

Proof. We have ax + py = 1 and bx' +py' =1. So ab(xx') + p(ybx' +y'ax +pyy') =1 and the theorem follows.

Theorem. For all primes p, for all integers a, b, if p|ab then p|a or p|b or both.

Proof If p|ab but not p|b and not p|a. Then we know gcd(p,a)=1 and gcd(p,b)=1. So gcd(p,ab)=1 contradicting p|ab.

Fact. (Unique Factorization Theorem) A composite integer m can be written in exactly one way as a product of the form

$$m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

where $p_1 < p_2 < \cdots < p_r$ are primes and e_i are positive integers.

Towards Euclid's Algorithm

- It follows from the Unique Factorization Theorem that if:

$$\begin{aligned} a &= p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \\ b &= p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r} \\ &\text{then} \\ gcd(a,b) &= p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_r^{\min(e_r,f_r)} \end{aligned}$$

Theorem For any nonnegative integers a and any positive integer b, gcd(a,b) = gcd(b, a mod b).

Proof Idea Show gcd(a,b)| gcd(b, a mod b) and gcd(b, a mod a) | gcd(a,b) using that gcd divides any linear combination of its arguments.

Euclid's Algorithm

- The theorem of the last slide can be converted into **Euclid's Algorithm** for finding gcd:

  Euclid(a,b) : if b=0 return a;
  else return Euclid(b, a mod b)

- **Example**:

  Euclid(99, 30) = Euclid(30, 9) = Euclid(9, 3) = Euclid(3,0) = 3.

Lemma

Lemma If a> b >=1 and the invocation Euclid(a,b) performs k>=1 recursive calls, then a >= F_{k+2} and b>= F_{k+1}. Here F_k is the kth Fibonacci number.

Proof By induction on k. Let k=1. Then b >=1 = F_2 and since a>b, a>=2 =F_3. So the statement is true. Since b > (a mod b), in each recursive call the first argument will always be the larger number.

Assume statement is true for k-1, then try to show for k. Suppose Euclid(a,b) performs k calls. Well, this function then call Euclid(b, a mod b) which then makes k-1 calls. By the induction hypothesis we have b>= $F_{(k-1)+2}$= F_{k+1} and a mod b >= F_k. Notice a >= b + (a mod b) >= F_{k+1}+ F_k = F_{k+2}.

Corollary (Lamé's Theorem) For any integer k>=1, if a>b>=1 and b< F_{k+1}**,** then the call Euclid(a,b) makes fewer than k recursive calls.

Extended Euclid

- Euclid's algorithm can be rewritten to get the x and y such that $ax+by = d = \gcd(a,b)$.

Extended-Euclid(a,b)

1. if $b=0$ then return $(a, 1, 0)$
2. $(d', x', y') =$ Extended-Euclid(b, a mod b)
3. $(d, x, y) = (d', y', x' - \lfloor a/b \rfloor y')$
4. return (d, x, y)

Modular Arithmetic

- We will be interested in exploiting the operations of + and * with respect to arithmetic modulo some integer.
- This kind of structure is called a **group**. Formally,

Definition A group $(S, \oplus)$ is a set together with a binary operation $\oplus$ defined on S for which the following properties hold:

1. **Closure**: For all a,b in S, $a \oplus b$ is in S.
2. **Identity**: There is an element e in S, called the **identity** of the group, such that $e \oplus a = a \oplus e = a$ for every a in S.
3. **Associativity**: For all a, b, c in S, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.
4. **Inverses**: For each a in S, there exists a unique element b in S, called the **inverse** of a, such that $a \oplus b = b \oplus a = e$.

Example (**Z**, +) is a group. If the set S is finite then the group is called a **finite group**. If the operation $\oplus$ is commutative then the group is called an **abelian group.**

Groups defined by modular arithmetic

- Recall from last day $[a]_n = \{a+kn \mid \text{for some integer } k\}$. This was an equivalence class for the equivalence relation b ~ a iff b-a = kn for some n. i.e., $b \equiv a \bmod n$.
- Let Z_n be the set $\{[b]_n \mid \text{for b an integer}\}$. Define $[a]_n+[b]_n = [a+b]_n$. Then last day, we argued on the board that $(Z_n, +)$ is a finite abelian group.
- Let Z_n^* be the set $\{[b]_n \mid \gcd(b,n) = 1\}$. Define $[a]_n*[b]_n = [a*b]_n$.

Theorem The system $(Z_n^*, *)$ is a finite abelian group.

Proof The set is obviously finite as it has fewer then n elements. Closure follows from Theorem (**) on an earlier slide. $[1]_n$ is easily seen to be an identity. To see the existence of inverses, let (d, x, y) be the output of Extended-Euclid(a, n). Then d=1 since a in Z_n^* so ax+ny=1. So $ax \equiv 1 \pmod n$. So x is a's inverse. Associativety and commutativety follow from these properties for **Z**.

More on Groups Defined by Modular Arithmetic

- We often are lazy and write b for the element $[b]_n$.
- We further write b^{-1} for the inverse of b mod n. For example, $-2 = (5)^{-1}$ mod 11.
- The size of Z_n^* is denoted by $\phi(n)$, called Euler's phi function.
- It satisfies the equation $$\phi(n) = n \prod_{p|n} (1 - 1/p)$$
- If (S, ⊕), then a subset S' of S that is also a group under ⊕, is called a subgroup of S.

Theorem. If (S, ⊕) is a finite group and S' is any nonempty set of S closed under ⊕, then (S', ⊕) is a subgroup of (S', ⊕).

Theorem. If (S, ⊕) is a finite group and (S', ⊕) is a subgroup, then |S'| is a divisor of S.