Divisibility

Aaron Pixton

June 11, 2010

1 Useful things

We write $d|n$ if d is a positive integer and $n = md$ for some integer m. Then let

$$d(n) := \sum_{d|n} 1 \text{ and } \sigma(n) := \sum_{d|n} d.$$

1.1 Primes

- Unique prime factorization: Any positive integer n can be uniquely written in the form

  $$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

  for primes $p_1 < \cdots < p_k$ and positive integers $a_1, \ldots, a_k$.

- Given the prime factorization of n, it is easy to compute $d(n)$ and $\sigma(n)$:

  $$d(n) = (a_1 + 1) \cdots (a_k + 1) \text{ and } \sigma(n) = \left(\frac{p_1^{a_1+1} - 1}{p_1 - 1} \right) \cdots \left(\frac{p_k^{a_k+1} - 1}{p_k - 1} \right).$$

- If p is prime and $p|ab$, then $p|a$ or $p|b$. Another way of stating this is that you can't write 0 as the product of two nonzero residues mod p.

- Finally, note that any integer greater than 1 has at least one prime divisor. As a sort of converse to this, if a positive integer has a divisor n, then it must be at least as large as n.

1.2 GCDs

- If m and n are integers, at least one nonzero, then they have a greatest common divisor $d := (m, n)$, the largest d such that $d|m$ and $d|n$.

- If the prime factorizations of m and n are known, then one can compute (m, n) easily: if $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, then $(m, n) = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$ with $c_i = \min(a_i, b_i)$.

- One useful fact is that $(m, n) = (m, n - m)$, or indeed $(m, n) = (m, n - km)$ for any integer k. If you repeat this to decrease the two numbers until one of them is zero, then this is the *Euclidean algorithm*.

- The Euclidean algorithm implies that there exist integers a and b such that $(m, n) = am + bn$. In fact, the diophantine equation $mx + ny = c$ (in x and y) only has a solution when c is a multiple of (m, n).

1.3 Exponentials

- Fermat's Little Theorem: if p is a prime and a is not divisible by p, then

$$p|a^{p-1}-1.$$

- Euler generalized this by introducing the function

$$\phi(n)=\sum_{\substack{1\le d\le n\\(d,n)=1}}1,$$

which counts the number of positive integers no larger than n that are relatively prime to n. Then Euler's generalization states that if $(a,n)=1$, then

$$n|a^{\phi(n)}-1.$$

- Note that if $n=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$, then

$$\frac{\phi(n)}{n}=\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

- As a consequence of Euler's generalization, the sequence $1,a,a^2,\ldots$ is periodic when reduced mod n, with period dividing $\phi(n)$.

2 Problems

1. Prove that there are infinitely many primes of the form $4n+3$.

2. (APMO 02) Find all positive integers a and b such that

$$\frac{a^2+b}{b^2-a}\text{ and }\frac{b^2+a}{a^2-b}$$

are both integers.

3. (ELMO 04) Let $a_0=n$ be a positive integer, and let $a_{i+1}=d(a_i)$ for $i\ge 0$. Find all n such that the sequence $a_0,a_1,\ldots$ does not contain any squares.

4. (Czech-Polish-Slovak 02) Let n be a positive integer and let p be a prime such that n divides $p-1$ and p divides n^3-1. Prove that $4p-3$ is a square.

5. Let $a_1=1$ and $a_{k+1}=2^{a_k}$ for each $k\ge 1$. Prove that $n|(a_{n+1}-a_n)$ for any positive integer n.

6. Let n be a positive integer that is not a perfect square and let m be a positive integer such that n divides $m-1$ and m divides n^3-1. Prove that $4m-3$ is a square.

7. Let $F_0=0,F_1=1$, and $F_{m+2}=F_{m+1}+F_m$ for $m\ge 0$. For which m,n is it the case that $F_m|F_n$?

8. (ISL 02/N3) Let $p_1,p_2,\ldots,p_n$ be distinct primes greater than 3. Show that $2^{p_1p_2\cdots p_n}+1$ has at least 4^n divisors. (Can you improve this bound?)

9. Find all positive integers n such that every prime divisor of 2^n-1 also divides 2^k-1 for some $0<k<n$.

10. (Romania TST 04) Let a,b be two positive integers, such that $ab\ne 1$. Find all the integer values that $f(a,b)$ can take, where

$$f(a,b)=\frac{a^2+ab+b^2}{ab-1}.$$

11. Find all positive integers n such that every prime divisor of the Fibonacci number F_n also divides some earlier Fibonacci number F_k $(0<k<n)$.