Disc Math - §7 - Elementary Number Theory

The Euclidean Algorithm

Def: Let $a,b\in\mathbb{Z}$ not both 0. The greatest common divisor of a and b denoted $\gcd(a,b)$ is the greatest integer n s.t. $n|a$ and $n|b$.

Integers a,b are relatively prime, if $\gcd(a,b)=1$.

Ex: $\gcd(72,-63)=9$; $\gcd(15,28)=1$ (rel. prime) ; $\gcd(a,0)=0$.

Lm: If $(a,b)\in\mathbb{Z}$ s.t. $(a,b)\neq(0,0)$ and $q,r\in\mathbb{Z}$ s.t. $a=bq+r$. Then

$$\gcd(a,b)=\gcd(b,r)$$

Pr: Let $\gcd(a,b)=d$. Since $r=a-bq \Rightarrow d|r \Rightarrow \gcd(a,b)\leq\gcd(b,r)$.

Let $\gcd(b,r)=d'$. Since $a=bq+r \Rightarrow d'|a \Rightarrow \gcd(b,r)\leq\gcd(a,b)$. ☒

Constr: (Euclidean Algorithm). (see binary GCD algorithm in the book).

Let $a,b\in\mathbb{Z}$ s.t. $a>b\geq 0$. To find $\gcd(a,b)$:

1. Check if $b=0$; if so $\gcd(a,b)=a$.
2. If not, compute the remainder of $a/b \to a=bq+r$, $0\leq r<b$
   $\gcd(a,b)=\gcd(b,r)$.
3. Repeat 2 until $r=0$.

Ex: $\gcd(222,156)=?$ $\quad 222=1\cdot156+66$, $156=2\cdot66+24$, $66=2\cdot24+18$,

$24=1\cdot18+6$, $18=3\cdot6+0$, $\gcd(222,156)=6$.

rem: notice that $\to$ $6=24-1(18)=24-1\cdot(66-2\cdot24)=3(24)-1(66)=$

$=3(156-2(66))-1(66)=3(156)-7(66)=3(156)-7(222-1(156))=$

$=10(156)-7(222)$.

Th: For $a,b\in\mathbb{Z}$, $(a,b)\neq(0,0)$. If $d=\gcd(a,b)$ Then $\exists m,n\in\mathbb{Z}$ s.t. $am+bn=d$

In fact $\gcd(a,b)=\min\{x=am+bn>0 \mid m,n\in\mathbb{Z}\}$. ☒ Proof above. Minic in the book.

Ex: Compute $\gcd(51,32)$ and express it as an integer combination of 51, 32

$51=1\cdot32+19$, $32=1\cdot(19)+13$, $19=1(13)+6$, $13=2(6)+1$, $6=6(1)+0$ $\quad\gcd=1$

$1=13-2(6)=13-2(19-1(13))=3(13)-2(19)=3(32-1(19))-2(19)=$

$=3(32)-5(19)=3(32)-5(51-32)=8(32)-5(51)$. $\qquad 1=8(32)-5(51)$.

Lm: Let $a,b \in \mathbb{Z}$ and p a prime number s.t $p \mid (ab)$. Then either $p \mid a$ or $p \mid b$.

Pr: If $p \mid a$ we are done. If $p \nmid a$ then since p is prime $\gcd(p,a)=1 \Rightarrow$ $\exists\, m,n \in \mathbb{Z}$ s.t. $1 = ma + np$. Multiplying this equation by b we have

$$b = mab + npb = m\,kp + npb = (mk+nb)p \Rightarrow p \mid b. \ \boxtimes$$

Cor: Let $a_1, a_2, \dots, a_k \in \mathbb{Z}$ and p be a prime number. Then if $p \mid (a_1 \cdots a_k)$ then $\exists\, j,\ 1 \le j \le k$ s.t. $p \mid a_j$. (Proof by e.g. induction).

Th: (Fundamental Theorem of Arithmetic) $\forall n \in \mathbb{N},\ n \ge 2$ is a prime number or can be written uniquely, up to reordering of the factors as a product of prime numbers.

Pr: We established before (in the section on induction) that $\forall n \in \mathbb{N}, n \ge 2$ is a prime number or a product of primes. So we just have to establish uniqueness.

Suppose that n can be factorized in two ways:

$$n = p_1 p_2 \cdots p_r \qquad p_1 \le p_2 \le \dots \le p_r \leftarrow \text{primes}$$

$$n = q_1 q_2 \cdots q_s \qquad q_1 \le q_2 \le \dots \le q_s \leftarrow \text{primes}$$

Then $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$.

Divide out the factors which are common on left and right. Let the remaining factors be $p_i' \cdots p_l' = q_1' \cdots q_j'$. By the previous corollary $\exists\, k$ s.t. $p_i' \mid q_k'$ and since these are prime $p_i' = q_k'$. But this is a contradiction since we eliminated the common factors. Thus the prime number factorization of n is unique.

Ex: $455 = 5 \cdot 91 = 5 \cdot 7 \cdot 13$; $680 = 2^3 \cdot 5 \cdot 17$

Ex: Find $\gcd(420, 66)$ by prime factorization.

$420 = 2^2 \cdot 3 \cdot 5 \cdot 7 \qquad 66 = 2 \cdot 3 \cdot 11 \qquad \gcd(420,66) = 2 \cdot 3 = 6.$

rem: For $n \in \mathbb{N}$ there is no "efficient" algorithm for discovering the prime factors of n.

Lm: If n is a composite integer, then it has a prime factor less than or equal to $\sqrt{n}$.

Pr: If $n = st$ then either s or $t \le \sqrt{n}$. ☒

Ex: $n = 1021$, $\sqrt{n} = 31.95$ Test division by $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 3$
None is a divisor → 1021 is prime.

rem: → By Euclid there are infinitely many primes; their distribution is highly erratic and not much is known.

→ As of Jan 2015, largest know prime is
$2^{57885161} - 1$ → 17 425 170 decimal digits (44km to write

→ The ten largest known primes are all Mersenne primes.

→ Goldbach conjecture (1742): Every even integer greater than 2 is the sum of two prime numbers (shown to hold up to 4×10^{18}).

Euler Phi Function. (Euler's Totient Function) (RSA encryption found.).

Def: For integer n, $n \ge 2$, the Euler phi function, $\varphi(n)$, is the number of positive integers $\le n$ which are relatively prime to n.

Ex: $\varphi(2) = 1$ $\{1\}$; $\varphi(3) = 2$ $\{1, 2\}$; $\varphi(4) = 2$ $\{1, 3\}$
$\varphi(5) = 4$ $\{1, 2, 3, 4\}$; $\varphi(6) = 2$ $\{1, 5\}$; $\varphi(7) = 6$ $\{1, 2, 3, 4, 5, 6\}$.

rem: If p is prime then $\varphi(p) = p - 1$.

constr: We will derive a formula for $\varphi(n)$. Let look at the case $n = p_1^{m_1} p_2^{m_2}$
To compute $\varphi(n)$ we will count all the positive integers $\le n$, or which there are n and throw out the ones that are not relatively prime to n
There are n/p_1 multiples of p_1 which are $\le n$ and also n/p_2 multiple of p_2 which are $\le n$, but n/p_1p_2 are multiples of both p_1 and p_2. Thus

$$\varphi(n) = n - \frac{n}{p_1} - \frac{n}{p_2} + \frac{n}{p_1 p_2} = n\left(\frac{p_1p_2 - p_1 - p_2 - 1}{p_1 p_2}\right) = \frac{n}{p_1 p_2}(p_1 - 1)(p_2 - 1) =$$

$\varphi(n) = p_1^{m_1-1} p_2^{m_2-1} \varphi(p_1)\varphi(p_2)$ $\boxtimes$

Th: If $n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$ is the prime factorization of n then

$$\varphi(n) = p_1^{m_1-1} p_2^{m_2-1} \dots p_k^{m_k-1} \varphi(p_1)\varphi(p_2)\dots\varphi(p_k). \quad \boxtimes$$

Ex: $n = 3150 = 2 \cdot 3^2 \cdot 5^2 \cdot 7$

$\varphi(n) = 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 1 \cdot 2 \cdot 4 \cdot 6 = 720$

HW p152, §2.4

2, 4, 10, 17, 20, 30, 40
45, 51