Introduction to number theory-3

April 3, 2017

Let $a_0, a_1, \ldots, a_N$ be real numbers with $a_i > 0$ for $i = 1, \ldots, N$. We define the *finite simple continued fraction*

$$\langle a_0, a_1, \ldots, a_N \rangle = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \, \cfrac{1}{a_{N-1} + \cfrac{1}{a_N}}}}}.$$

Another notation for a continued fraction is

$$\langle a_0, a_1, \ldots, a_N \rangle = a_0 + \frac{1}{a_1+}\,\frac{1}{a_2+} \cdots \frac{1}{a_N}.$$

The numbers $a_0, a_1, \ldots, a_N$ are called the *partial quotients* of the continued fraction.

We can write a finite simple continued fraction as a rational function in the variables $a_0, a_1, \ldots, a_N$. For example,

$$\langle a_0 \rangle = a_0, \qquad \langle a_0, a_1 \rangle = \frac{a_0 a_1 + 1}{a_1}, \quad \langle a_0, a_1, a_2 \rangle = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1}.$$

and

If $N \geq 1$, then $\langle a_0, a_1, \ldots, a_N \rangle = a_0 + \dfrac{1}{\langle a_1, \ldots, a_N \rangle}$.

We can use the Euclidean algorithm to write a rational number as a finite simple continued fraction with integral partial quotients. For example, to represent 574/274, we have

$$\begin{aligned}\frac{574}{252} &= 2+\frac{70}{252} = 2+\frac{1}{3+\frac{42}{70}} = 2+\frac{1}{3+\frac{1}{1+\frac{28}{42}}} = \\ &= 2+\frac{1}{3+\frac{1}{1+\frac{1}{1+\frac{1}{2}}}} = \langle 2,3,1,1,2\rangle.\end{aligned}$$

$$\boxed{\begin{aligned} 574 &= 252\cdot 2 + 70, \\ 252 &= 70\cdot 3 + 42, \\ 70 &= 42\cdot 1 + 28, \\ 42 &= 28\cdot 1 + 14, \\ 28 &= 14\cdot 2\,. \end{aligned}}$$

Notice that the partial quotients in the Euclidean algorithm are the partial quotients in the continued fraction.

Theorem 1.6 *Let a and b be integers with $b \geq 1$. If the Euclidean algorithm for a and b has length n with sequence of partial quotients $q_0, q_1, \ldots, q_{n-1}$, then*

$$\frac{a}{b} = \langle q_0, q_1, \ldots, q_{n-1} \rangle.$$

Proof. Let $r_0 = a$ and $r_1 = b$. The proof is by induction on n. If $n = 1$,

$$\text{then} \quad r_0 = r_1 q_0 \qquad \text{and} \qquad \frac{a}{b} = \frac{r_0}{r_1} = q_0 = \langle q_0 \rangle.$$

If $n = 2$, then
$$\begin{aligned} r_0 &= r_1 q_0 + r_2, \quad \text{and} \\ r_1 &= r_2 q_1, \end{aligned}$$
$$\frac{a}{b} = \frac{r_0}{r_1} = q_0 + \frac{r_2}{r_1} = q_0 + \frac{1}{\frac{r_1}{r_2}} = q_0 + \frac{1}{q_1} = \langle q_0, q_1 \rangle.$$

Let $n \geq 2$, and assume that the theorem is true for integers a and $b \geq 1$ whose Euclidean algorithm has length n. Let a and $b \geq 1$ be integers whose Euclidean algorithm has length $n + 1$ and whose sequence of partial quotients is $\langle q_0, q_1, \ldots, q_n \rangle$.

Let
$$\begin{aligned} r_0 &= r_1 q_0 + r_2 \\ r_1 &= r_2 q_1 + r_3 \\ &\vdots \\ r_{n-1} &= r_n q_{n-1} + r_{n+1} \\ r_n &= r_{n+1} q_n . \end{aligned}$$

be the $n+1$ equations in the Euclidean algorithm for $a = r_0$ and $b = r_1$. The Euclidean algorithm for the positive integers r_1 and r_2 has length n with sequence of partial quotients $q_1, \ldots, q_n$. It follows from the induction hypothesis that

$$\frac{r_1}{r_2} = \langle q_1, \ldots, q_n \rangle$$

and so
$$\frac{a}{b} = \frac{r_0}{r_1} = q_0 + \frac{1}{\frac{r_1}{r_2}} = q_0 + \frac{1}{\langle q_1, \ldots, q_n \rangle} = \langle q_0, q_1, \ldots, q_n \rangle .$$

This completes the proof.

It is also true that the representation of a rational number as a finite simple continued fraction is essentially unique.

The Fundamental Theorem of Arithmetic

A *prime number* is an integer p greater than 1 whose only positive divisors are 1 and p. A positive integer greater than 1 that is not prime is called *composite*. If n is composite, then it has a divisor d such that $1 < d < n$, and so $n = dd'$, where also $1 < d' < n$. The primes less than 100 are the following:

$$\begin{array}{rrrrr}
2 & 3 & 5 & 7 & 11 \\
13 & 17 & 19 & 23 & 29 \\
31 & 37 & 41 & 43 & 47 \\
53 & 59 & 61 & 67 & 71 \\
73 & 79 & 83 & 89 & 97.
\end{array}$$

If d is a positive divisor of n, then $d' = n/d$ is called the *conjugate divisor* to d. If $n = dd'$ and $d \leq d'$, then $d \leq \sqrt{n}$.

We shall prove that every positive integer can be written as the product of prime numbers (with the convention that the empty product is equal to 1), and that this representation is unique except for the order in which the prime factors are written. This result is called the *fundamental theorem of arithmetic*.

Theorem 1.7 (Euclid's lemma) *Let a, b, c be integers. If a divides bc and $(a, b) = 1$, then a divides c.*

Proof. Since a divides bc, we have $bc = aq$ for some integer q. Since a and b are relatively prime, Theorem 1.5 implies that there exist integers x and y such that

$$1 = ax + by.$$

Multiplying by c, we obtain

$$c = acx + bcy = acx + aqy = a(cx + qy),$$

and so a divides c. This completes the proof.

Theorem 1.8 *Let $k \geq 2$, and let $a, b_1, b_2, \ldots, b_k$ be integers. If $(a, b_i) = 1$ for all $i = 1, \ldots, k$, then $(a, b_1 b_2 \cdots b_k) = 1$.*

Proof. The proof is by induction on k. Let $k = 2$ and $d = (a, b_1 b_2)$. We must show that $d = 1$. Since d divides a and $(a, b_1) = 1$, it follows that $(d, b_1) = 1$. Since d divides $b_1 b_2$, Euclid's lemma implies that d divides b_2. Therefore, d is a common divisor of a and b_2, but $(a, b_2) = 1$ and so $d = 1$.

Let $k \geq 3$, and assume that the result holds for $k - 1$. Let $a, b_1, \ldots, b_k$ be integers such that $(a, b_i) = 1$ for $i = 1, \ldots, k$. The induction assumption implies that $(a, b_1 \cdots b_{k-1}) = 1$. Since we also have $(a, b_k) = 1$, it follows from the case $k = 2$ that $(a, b_1 \cdots b_{k-1} b_k) = 1$. This completes the proof.

Theorem 1.9 *If a prime number p divides a product of integers, then p divides one of the factors.*

Proof. Let $b_1, b_2, \ldots, b_k$ be integers such that p divides $b_1 \cdots b_k$. By Theorem 1.8, we have $(p, b_i) > 1$ for some i. Since p is prime, it follows that p divides b_i. □

Theorem 1.10 (Fundamental theorem of arithmetic) *Every positive integer can be written uniquely (up to order) as the product of prime numbers.*

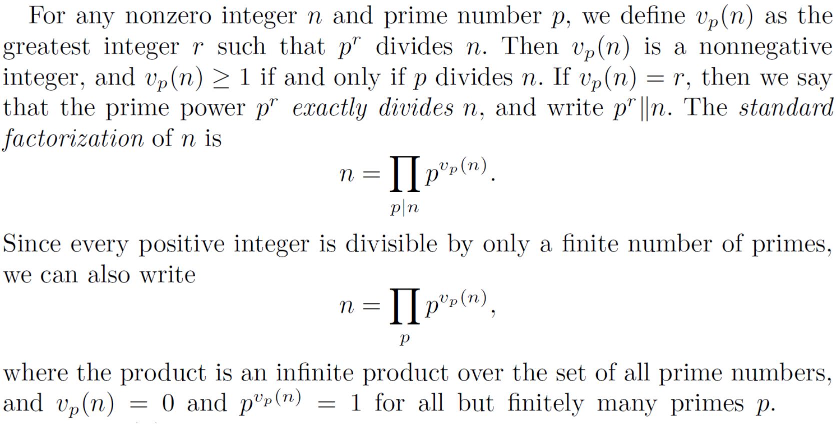
Proof. First we prove that every positive integer can be written as a product of primes. Since an empty product is equal to 1, we can write 1 as the empty product of primes. Let $n \geq 2$. Suppose that every positive integer less than n is a product of primes. If n is prime, we are done. If n is composite, then $n = dd'$, where $1 < d \leq d' < n$. By the induction hypothesis, d and d' are both products of primes, and so $n = dd'$ is a product of primes.

Next we use induction to prove that this representation is unique. The representation of 1 as the product of the empty set of primes is unique. Let $n \geq 2$ and assume that the statement is true for all positive integers less than n. We must show that if $n = p_1 \cdots p_k = p'_1 \cdots p'_\ell$, where $p_1, \ldots, p_k, p'_1, \ldots, p'_\ell$ are primes, then $k = \ell$ and there is a permutation σ of $1, \ldots, k$ such that $p_i = p'_{\sigma(i)}$ for $i = 1, \ldots, k$. By Theorem 1.9, since p_k divides $p'_1 \cdots p'_\ell$, there exists an integer $j_0 \in \{1, \ldots, \ell\}$ such that p_k divides p'_{j_0}, and so $p_k = p'_{j_0}$ since p'_{j_0} is prime. Therefore,

$$\frac{n}{p_k} = p_1 \cdots p_{k-1} = \prod_{\substack{j=1 \\ j \neq j_0}}^{\ell} p'_j < n.$$

It follows from the induction hypothesis that $k-1=\ell-1$, and there is a one-to-one map σ from $\{1,\ldots,k-1\}$ into $\{1,\ldots,k\}\setminus\{j_0\}$ such that $p_i=p'_{\sigma(i)}$ for $i=1,\ldots,k-1$. Let $\sigma(k)=j_0$. This defines the permutation σ, and the proof is complete.

p-adic value



For any nonzero integer n and prime number p, we define $v_p(n)$ as the greatest integer r such that p^r divides n. Then $v_p(n)$ is a nonnegative integer, and $v_p(n) \geq 1$ if and only if p divides n. If $v_p(n) = r$, then we say that the prime power p^r *exactly divides* n, and write $p^r \| n$. The *standard factorization* of n is

$$n = \prod_{p|n} p^{v_p(n)}.$$

Since every positive integer is divisible by only a finite number of primes, we can also write

$$n = \prod_{p} p^{v_p(n)},$$

where the product is an infinite product over the set of all prime numbers, and $v_p(n) = 0$ and $p^{v_p(n)} = 1$ for all but finitely many primes p.

p-adic value

The function $v_p(n)$ is called the *p-adic value of* n.

It is *completely additive* in the sense that $v_p(mn) = v_p(m) + v_p(n)$ for all positive integers m and n For example, since $n! = 1 \cdot 2 \cdot 3 \cdots n$, we have

$$v_p(n!) = \sum_{m=1}^{n} v_p(m).$$

common multiple

Let $a_1, \ldots, a_k$ be nonzero integers. An integer m' is called a *common multiple* of $a_1, \ldots, a_k$ if it is a multiple of a_i for all $i = 1, \ldots, k$, that is, every integer a_i divides m'. The *least common multiple* of $a_1, \ldots, a_k$ is a positive integer m such that m is a common multiple of $a_1, \ldots, a_k$, and m divides every common multiple of $a_1, \ldots, a_k$. For example, 910 is a common multiple of 35 and 91, and 455 is the least common multiple. We shall show that there is a unique least common multiple for every finite set of nonzero integers. We denote by $[a_1, \ldots, a_k]$ the least common multiple of $a_1, \ldots, a_k$.

Theorem 1.11 *Let $a_1, \ldots, a_k$ be positive integers. Then*

$$(a_1, \ldots, a_k) = \prod_p p^{\min\{v_p(a_1), \ldots, v_p(a_k)\}}$$

and

$$[a_1, \ldots, a_k] = \prod_p p^{\max\{v_p(a_1), \ldots, v_p(a_k)\}}.$$

Proof. This follows immediately from the fundamental theorem of arithmetic. □

Let x be a real number. Recall that the *integer part* of x is the greatest integer not exceeding x, that is, the unique integer n such that $n \leq x < n+1$. We denote the integer part of x by $[x]$. For example, $\left[\frac{4}{3}\right] = 1$, $[\sqrt{7}] = 2$, and $\left[-\frac{4}{3}\right] = -2$. The *fractional part* of x is the real number

$$\{x\} = x - [x] \in [0, 1).$$

Thus, $\left\{\frac{4}{3}\right\} = \frac{1}{3}$ and $\left\{-\frac{4}{3}\right\} = \frac{2}{3}$. We can use the greatest integer function to compute the standard factorization of factorials.

Theorem 1.12 *For every positive integer n and prime p,*

$$v_p(n!) = \sum_{r=1}^{\left[\frac{\log n}{\log p}\right]} \left[\frac{n}{p^r}\right].$$

Proof. Let $1 \leq m \leq n$. If p^r divides m, then $p^r \leq m \leq n$ and $r \leq \log n / \log p$. Since r is an integer, we have $r \leq [\log n / \log p]$ and

$$v_p(m) = \sum_{\substack{r=1 \\ p^r \mid m}}^{\left[\frac{\log n}{\log p}\right]} 1.$$

The number of positive integers not exceeding n that are divisible by p^r is exactly $[n/p^r]$, and so

$$\begin{aligned} v_p(n!) &= \sum_{m=1}^{n} v_p(m) = \sum_{m=1}^{n} \sum_{\substack{r=1 \\ p^r \mid m}}^{\left[\frac{\log n}{\log p}\right]} 1 \\ &= \sum_{r=1}^{\left[\frac{\log n}{\log p}\right]} \sum_{\substack{m=1 \\ p^r \mid m}}^{n} 1 = \sum_{r=1}^{\left[\frac{\log n}{\log p}\right]} \left[\frac{n}{p^r}\right]. \end{aligned}$$

This completes the proof.

We shall use Theorem 1.12 to compute the standard factorization of 10!. The primes not exceeding 10 are $2, 3, 5$, and 7, and

$$v_2(10!) = \left[\frac{10}{2}\right] + \left[\frac{10}{4}\right] + \left[\frac{10}{8}\right] = 5 + 2 + 1 = 8,$$

$$v_3(10!) = \left[\frac{10}{3}\right] + \left[\frac{10}{9}\right] = 4,$$

$$v_5(10!) = \left[\frac{10}{5}\right] = 2,$$

$$v_7(10!) = \left[\frac{10}{7}\right] = 1.$$

Therefore,

$$10! = 2^8 3^4 5^2 7.$$

For every nonzero integer m, the *radical of* m, denoted by $\mathrm{rad}(m)$, is the product of the distinct primes that divide m, that is,

$$\mathrm{rad}(m) = \prod_{p|m} p = \prod_{v_p(m)\geq 1} p.$$

For example, $\mathrm{rad}(15) = \mathrm{rad}(-45) = \mathrm{rad}(225) = 15$ and $\mathrm{rad}(p^r) = p$ for p prime and $r \geq 1$.

Theorem 1.13 *Let m and a be nonzero integers. There exists a positive integer k such that m divides a^k if and only if rad(m) divides rad(a).*

Proof. We know that m divides a^k if and only if $v_p(m) \leq v_p(a^k) = kv_p(a)$ for every prime p. If there exists an integer k such that m divides a^k, then $v_p(a) > 0$ whenever $v_p(m) > 0$, and so every prime that divides m also divides a. This implies that $\text{rad}(m)$ divides $\text{rad}(a)$.

Conversely, if $\text{rad}(m)$ divides $\text{rad}(a)$, then $v_p(a) > 0$ for every prime p such that $v_p(m) > 0$. Since only finitely many primes divide m, it follows that there exists a positive integer k such that $v_p(a^k) = kv_p(a) \geq v_p(m)$ for all primes p, and so m divides a^k.

Euclid's Theorem and the Sieve of Eratosthenes

Theorem 1.14 (Euclid's theorem) *There are infinitely many primes.*

Proof. Let $p_1, \ldots, p_n$ be any finite set of prime numbers. Consider the integer

$$N = p_1 \cdots p_n + 1.$$

Since $N > 1$, it follows from the fundamental theorem of arithmetic that N is divisible by some prime p. If $p = p_i$ for some $i = 1, \ldots, n$, then p divides $N - p_1 \cdots p_n = 1$, which is absurd. Therefore, $p \neq p_i$ for all $i = 1, \ldots, n$. This means that, for any finite set of primes, there always exists a prime that does not belong to the set, and so the number of primes is infinite.

Let $\pi(x)$ denote the number of primes not exceeding x. Then $\pi(x) = 0$ for $x < 2$, $\pi(x) = 1$ for $2 \leq x < 3$, $\pi(x) = 2$ for $3 \leq x < 5$, and so on. Euclid's theorem says that there are infinitely many prime numbers, that is,

$$\lim_{x\to\infty} \pi(x) = \infty,$$

but it does not tell us how to determine them. We can compute all the prime numbers up to x by using a beautiful and efficient method called the *sieve of Eratosthenes*. The sieve is based on a simple observation. If the positive integer n is composite, then n can be written in the form $n = dd'$, where $1 < d \leq d' < n$. If $d > \sqrt{n}$, then

$$n = dd' > \sqrt{n}\sqrt{n} = n,$$

which is absurd. Therefore, if n is composite, then n has a divisor d such that $1 < d \leq \sqrt{n}$. In particular, every composite number $n \leq x$ is divisible by a prime $p \leq \sqrt{x}$.

To find all the primes up to x, we write down the integers between 1 and x, and eliminate numbers from the list according to the following rule: Cross out 1. The first number in the list that is not eliminated is 2; cross out all multiples of 2 that are greater than 2. The iterative procedure is as follows: Let d be the smallest number on the list whose multiples have not already been eliminated. If $d \leq \sqrt{x}$, then cross out all multiples of d that are greater than d. If $d > \sqrt{x}$, stop. This algorithm must terminate after at most $\sqrt{x}$ steps. The prime numbers up to x are the numbers that have not been crossed out.

We shall demonstrate this method to find the prime numbers up to 60. We must sieve out by the prime numbers less than $\sqrt{60}$, that is, by $2, 3, 5$, and 7. We cross out 1 and all multiples of 2 beginning with 4:

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	55	~~56~~	~~57~~	~~58~~	59	~~60~~

Next we cross out all multiples of 5 beginning with 10:

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~

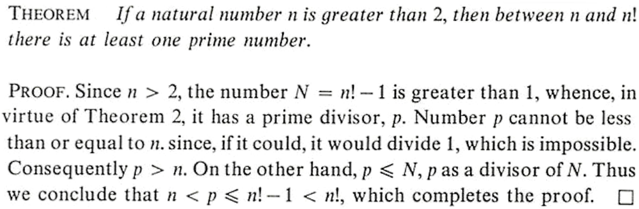
Finally, we cross out all multiples of 7 beginning with 14:

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~

The numbers that have not been crossed out are:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59.$$

These are the prime numbers up to 60.



THEOREM *If a natural number n is greater than 2, then between n and $n!$ there is at least one prime number.*

PROOF. Since $n > 2$, the number $N = n! - 1$ is greater than 1, whence, in virtue of Theorem 2, it has a prime divisor, p. Number p cannot be less than or equal to n. since, if it could, it would divide 1, which is impossible. Consequently $p > n$. On the other hand, $p \leqslant N$, p as a divisor of N. Thus we conclude that $n < p \leqslant n! - 1 < n!$, which completes the proof. □