Proseminar: How to solve it?

Numbertheory: Primes and (simultaneous) congruences

Martin Suderland, Daniel Rosenblüh

It is known that for every positive integer a, there is a unique expression $a = p_1^{m_1} p_2^{m_2} \cdot \ldots \cdot p_r^{m_r} = \prod_{k=1}^{r} p_k^{m_k}$ with primes $p_1 < p_2 < \cdots < p_r$ and exponents $m_1 \geq 1, \ldots, m_r \geq 1$. This is called the fundamental theorem of arithmetic.

First we will give an (interesting) proof to show that there are infinitely many primes.

Theorem 1 (Infiniteness of primes) *The series of the reciprocals of the primes* $\sum_{p \in \mathbb{P}} \frac{1}{p}$ *diverges. Therefore, the number of primes is infinite.*

Proof. Assume that $\sum_{p \in \mathbb{P}} \frac{1}{p}$ converges. Then there must be a natural number k such that $\sum_{i \geq k+1} \frac{1}{p_i} < \frac{1}{2}$ with $p_1, p_2, p_3, \ldots$ being the sequence of primes in increasing order. Let's call $p_1, \ldots, p_k$ the small primes and $p_{k+1}, p_{k+2}, \ldots$ the big primes. For every natural number N there is

$$\sum_{i \geq k+1} \frac{N}{p_i} < \frac{N}{2}.$$

We define N_b as the number of positive integers $n \leq N$ which are divisible by at least one big prime and N_s as the number of positive integers $n \leq N$ which have only small prime divisors. We are going to show that there exists an N such that $N_s + N_b < N$ which is the desired contradiction, since by definition $N_s + N_b$ equals N.

As we know $\left\lfloor \frac{N}{p_i} \right\rfloor$ counts the positive integers $n \leq N$ which are multiples of p_i. Hence by the above equation we obtain

$$N_b \leq \sum_{i \geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor < \frac{N}{2}.$$

Now we'll have a look at N_s. We write every $n \leq N$ which has only small prime divisors in the form $n = a_n b_n^2$ where a_n is the square-free part. Thus every a_n is a product of different small primes. By the product rule in combinatorics there exist

exactly 2^k different square-free parts. Furthermore, as $b_n \leq \sqrt{n} \leq \sqrt{N}$, we find that there are at most $\sqrt{N}$ different square parts, so $N_s \leq 2^k\sqrt{N}$. Now choose $N = 2^{2k+2}$:

$$N_b + N_s < \frac{N}{2} + 2^k\sqrt{N} = 2^{2k+1} + 2^k \cdot 2^{k+1} = 2^{2k+2} = N.$$

□

It can be shown that the series of the reciprocals of the twin primes

$$\sum_{p,p+2\in\mathbb{P}} \left(\frac{1}{p} + \frac{1}{p+2}\right)$$

converges. If the series diverged, this would prove that there are infinitely many twin primes.

Definition 2 (The sum of all positive divisors) *For every natural number a we call $\sigma(a)$ the sum of all positive divisors of a. We write*

$$\sigma(a) = \sum_{d|a} d.$$

Theorem 3 *Let $a = p_1^{m_1} p_2^{m_2} \cdot \ldots \cdot p_r^{m_r}$, then*

$$\sigma(a) = \prod_{k=1}^{r} \frac{p_k^{m_k+1} - 1}{p_k - 1}, \qquad \textit{particulary } \sigma\left(\prod_{k=1}^{r} p_k^{m_k}\right) = \prod_{k=1}^{r} \sigma\left(p_k^{m_k}\right).$$

Proof. The positive divisors of a are exactly all numbers $p_1^{n_1} p_2^{n_2} \cdot \ldots \cdot p_r^{n_r}$ with $0 \leq n_k \leq m_k, \quad k = 1, \ldots, r$. Their sum is

$$\sigma(a) = \sum_{n_1,\ldots,n_r=0}^{m_1,\ldots,m_r} p_1^{n_1} p_2^{n_2} \cdot \ldots \cdot p_r^{n_r} = \sum_{n_1=0}^{m_1} \sum_{n_2=0}^{m_2} \cdots \sum_{n_r=0}^{m_r} p_1^{n_1} p_2^{n_2} \cdot \ldots \cdot p_r^{n_r}.$$

The right term can be written as

$$\sigma(a) = \left(\sum_{n_1=0}^{m_1} p_1^{n_1}\right)\left(\sum_{n_2=0}^{m_2} p_2^{n_2}\right) \cdot \ldots \cdot \left(\sum_{n_r=0}^{m_r} p_r^{n_r}\right) = \prod_{k=1}^{r} \left(\sum_{n_k=0}^{m_k} p_k^{n_k}\right)$$

The factors of the product are geometric series

$$\sum_{n_k=0}^{m_k} p_k^{n_k} = \frac{p_k^{m_k+1} - 1}{p_k - 1}. \qquad \text{Inserting in the last equation gives } \sigma(a) = \prod_{k=1}^{r} \frac{p_k^{m_k+1} - 1}{p_k - 1}.$$

□

Definition 4 (Perfect numbers) *A natural number a is called a "perfect number" if $\sigma(a) = 2a$.*

All even perfect numbers can be precisely defined. We show the following theorem.

Theorem 5 (Characterization of even perfect numbers) *The following statements about a natural number $a = 2^{s-1}b$, $s \geq 2$, b odd, are equivalent:*

i) b is prime, and $b = 2^s - 1$

ii) a is perfect

Proof. i) $\Rightarrow$ ii): According to the assumption, $b \neq 2$ is prime and therefore $a = 2^{s-1}b$ is the prime factorization of a. Applying theorem 3 yields:

$$\sigma(a) = \frac{2^s - 1}{2 - 1} \cdot \frac{b^2 - 1}{b - 1} = (2^s - 1)\,(b + 1).$$

Since $b + 1 = 2^s = 2 \cdot 2^{s-1}$ according to the assumption, it follows that

$$\sigma(a) = 2 \cdot 2^{s-1} \cdot (2^s - 1) = 2a.$$

ii) $\Rightarrow$ i): Since b is odd, all prime factors of b are $\neq 2$. From theorem 3 follows:

$$2a = 2 \cdot 2^{s-1} \cdot b = 2^s b = 2a = \sigma(a) = \sigma\left(2^{s-1}\right) \cdot \sigma(b) = (2^s - 1)\,\sigma(b).$$

This implies:

$$\sigma(b) = \frac{2^s}{2^s - 1} b = b + c \quad \text{with} \quad c := \frac{b}{2^s - 1}.$$

Since $b \in \mathbb{N}$, $\sigma(b) \in \mathbb{N}$ and $\sigma(b) > b$, for c there is $c \in \mathbb{N}$. From the equation $b = c(2^s - 1)$ follows that c is a divisor of b. Since $\sigma(b) = b + c$, b and c are the only (two) divisors of b. Therefore b must be prime and $c = 1$. From the definition of c follows that $b = 2^s - 1$.

□

It is not known if there is any odd perfect number. If there is, it has to be greater than 10^{300}.

We already know Euler's totient function $\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$ which tells you how many numbers in $\{1, \ldots, n\}$ are coprime to n. One example where Euler's totient function is used, is the following theorem.

Theorem 6 (Euler theorem) *If a and m are positive integers and* $\gcd(a, m) = 1$, *then*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Proof. Let $r_1, r_2, \ldots, r_n$ be the coprime numbers to m between 1 and m. This implies $\varphi(m) = n$. Choose a natural number a which is relatively prime to m. Have a look at the numbers $ar_1, ar_2, \ldots, ar_n$ They obviously have no common prime factor with m. Moreover they are relatively incongruent, because $ar_i \equiv ar_j \pmod{m} \Rightarrow r_i \equiv r_j \pmod{m}$ by multiplying with the inverse of a. We can conclude that

$$r_1 \cdot \ldots \cdot r_n \equiv ar_1 \cdot \ldots \cdot ar_n \pmod{m}.$$

Because $r_1, r_2, \ldots, r_n$ are coprime to m their product must be as well. So we are allowed to divide the above equation by it. It follows that $1 \equiv a^n \pmod{m}$ or

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

□

The Euler theorem is a generalization of Fermat's little theorem, since for $p \in \mathbb{P}$, $\varphi(p) = p - 1$ and therefore $a^{p-1} \equiv 1 \pmod{p}$.

Theorem 7 (Chinese remainder theorem) *Let $n_1, \ldots, n_k$ be positive, pairwise relatively prime integers and let $a_1, \ldots, a_k$ be arbitrary integers. Then there exists a solution $a \in \mathbb{Z}$ to the system of congruences*

$$a \equiv a_i \pmod{n_i} \quad (i = 1, \ldots, k).$$

Moreover, any $a' \in \mathbb{Z}$ is a solution if and only if $a' \equiv a \pmod{n}$ with $n := \prod_{i=1}^{k} n_i$.

Proof. To prove the existence of a solution a to the system of congruences we will first show how to construct integers $e_1, \ldots, e_k$ satisfying

$$e_j \equiv \begin{cases} 1 \pmod{n_i} & \text{if } j = i \\ 0 \pmod{n_i} & \text{if } j \neq i \end{cases}$$

with $i, j = 1, \ldots, k$.

Then setting $a := \sum_{i=1}^{k} a_i e_i$, it is easy to verify that $a = \sum_{i=1}^{k} a_i e_i \equiv a_j \pmod{n_j}$ applies for all $j \in \{1, \ldots, k\}$ since all but one of the terms of the sum are zero modulo n_j (by definition of e_j). To find $e_1, \ldots, e_k$ satisfying the above equation, let $n_i^* := n/n_i = \prod_{j \neq i} n_j$. Since all elements of the set $\{n_1, \ldots, n_k\}$ are coprime to each other, we know that $\gcd(n_i, n_i^*) = 1$ for all $i \in \{1, \ldots, k\}$. So there exist t_i with $t_i n_i^* \equiv 1 \pmod{n_i}$. With $e_i = t_i n_i^*$, we have $e_i \equiv 1 \pmod{n_j}$ for $i = j$, and in the case $i \neq j$ we have $e_i \equiv 0 \pmod{n_j}$ since n_i^* contains all factors n_j (with $i \neq j$).

That proves the existence of a solution $a \in \mathbb{Z}$ to the system of congruences. Moreover, $a' \equiv a \pmod{n}$ is a solution, because from $n_i \mid n$ for all $i \in \{1, \ldots, k\}$ follows that $a' \equiv a \equiv a_i \pmod{n_i}$ for all $i \in \{1, \ldots, k\}$.

To prove the uniqueness, we assume a'' is a solution to the system of congruences. Then $a \equiv a_i \equiv a'' \pmod{n_i}$ for all $i \in \{1, \ldots, k\}$. Therefore $n_i \mid a - a''$ for all $i \in \{1, \ldots, k\}$ and since all elements of the set $\{n_1, \ldots, n_k\}$ are relatively prime to each other, it follows that $n \mid a - a''$ or more specifically $a'' \equiv a \pmod{n}$.

□

Exercises 8 *1. Find the eight last digits of the binary expansion of* 27^{1986}.

2. For any integer a, *set* $n_a = 101a - 100 \cdot 2^a$. *Show that for* $0 \leq a, b, c, d \leq 99$,

$$n_a + n_b \equiv n_c + n_d \pmod{101000}$$

implies $\{a, b\} = \{c, d\}$.

3. Show that there exist 2010 consecutive numbers, each of which is divisible by the cube of an integer.