MATH 433

Applied Algebra

Lecture 5:
Prime factorisation (continued).
Congruences.

Prime factorisation

A positive integer *p* is **prime** if it has exactly two positive divisors, namely, 1 and *p*.

Prime factorisation of a positive integer $n \geq 2$ is a decomposition of *n* into a product of primes.

Theorem Any positive integer $n \geq 2$ admits a prime factorisation. This factorisation is unique up to rearranging the factors.

Fermat and Mersenne primes

Proposition For any integer $k \geq 2$ and any $x, y \in \mathbb{R}$,

$$x^k - y^k = (x-y)(x^{k-1} + x^{k-2}y + \cdots + xy^{k-2} + y^{k-1}).$$

If, in addition, k is odd, then

$$x^k + y^k = (x+y)(x^{k-1} - x^{k-2}y + \cdots - xy^{k-2} + y^{k-1}).$$

Corollary 1 (Mersenne) The number $2^n - 1$ is composite whenever n is composite.

(Hint: use the first formula with $x = 2^{n/k}$, $y = 1$, and k a prime divisor of n.)

Corollary 2 (Fermat) Let $n \geq 2$ be an integer. Then the number $2^n + 1$ is composite whenever n is not a power of 2.

(Hint: use the second formula with $x = 2^{n/k}$, $y = 1$, and k an odd prime divisor of n.)

Mersenne primes are primes of the form $2^p - 1$, where p is prime. **Fermat primes** are primes of the form $2^{2^n} + 1$.

Let $a = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$ and $b = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$, where $p_1, p_2, \dots, p_k$ are distinct primes and n_i, m_i are nonnegative integers.

Theorem **(i)** $ab = p_1^{n_1+m_1} p_2^{n_2+m_2} \dots p_k^{n_k+m_k}$.

(ii) a divides b if and only if $n_i \le m_i$ for $i = 1, 2, \dots, k$.

(iii) $\gcd(a, b) = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$, where $s_i = \min(n_i, m_i)$.

(iv) $\mathrm{lcm}(a, b) = p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}$, where $t_i = \max(n_i, m_i)$.

Corollary $\gcd(a, b) \cdot \mathrm{lcm}(a, b) = ab$.

Problem. When the number $14^7 \cdot 25^{30} \cdot 40^{12}$ is written out, how many consecutive zeroes are there at the right-hand end?

The number of consecutive zeroes at the right-hand end is the exponent of the largest power of 10 that divides our number.

As follows from the Unique Factorisation Theorem, a positive integer A divides another positive integer B if and only if the prime factorisation of A is part of the prime factorisation of B.

The prime factorisation of the given number is

$$14^7 \cdot 25^{30} \cdot 40^{12} = (2 \cdot 7)^7 \cdot (5^2)^{30} \cdot (2^3 \cdot 5)^{12} = 2^{43} \cdot 5^{72} \cdot 7^7.$$

For any integer $n \geq 1$ the prime factorisation of 10^n is $2^n{\cdot}5^n$.

Hence 10^n divides the given number if $n \leq 43$ and $n \leq 72$. The largest number with this property is 43. Thus there are 43 zeroes at the right-hand end.

Congruences

Let n be a positive integer. The integers a and b are called **congruent modulo** n if they have the same remainder when divided by n. An equivalent condition is that n divides the difference $a - b$.

Notation. $a \equiv b \bmod n$ or $a \equiv b \pmod{n}$.

Examples. $12 \equiv 4 \bmod 8$, $24 \equiv 0 \bmod 6$, $31 \equiv -4 \bmod 35$.

Proposition If $a \equiv b \bmod n$ then for any integer c,
(i) $a + cn \equiv b \bmod n$;
(ii) $a + c \equiv b + c \bmod n$;
(iii) $ac \equiv bc \bmod n$.

Indeed, if $a - b = kn$, where k is an integer, then
$(a + cn) - b = a - b + cn = (k + c)n$,
$(a + c) - (b + c) = a - b = kn$, and
$ac - bc = (a - b)c = (kc)n$.

Problem. Prove that the number 2023 cannot be expressed as the sum of two squares (of integers).

The key idea is to look at the remainder after division by 4. We have $2023 \equiv 3 \bmod 4$.

Now let $n = a^2 + b^2$, where $a, b \in \mathbb{Z}$. If a and b are both even, then $n = (2k)^2 + (2m)^2 = 4(k^2 + m^2)$ so that $n \equiv 0 \bmod 4$.

If a and b are both odd, then $n = (2k+1)^2 + (2m+1)^2 = 4(k^2 + k + m^2 + m) + 2$ so that $n \equiv 2 \bmod 4$.

If one of the numbers a and b is even and one is odd, then $n = (2k)^2 + (2m+1)^2 = 4(k^2 + m^2 + m) + 1$ so that $n \equiv 1 \bmod 4$.

Thus the equation $a^2 + b^2 = 2023$ has no integer solutions since the congruency $a^2 + b^2 \equiv 2023 \bmod 4$ has no solution.

More properties of congruences

Proposition If $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$, then **(i)** $a + b \equiv a' + b' \bmod n$;
(ii) $a - b \equiv a' - b' \bmod n$;
(iii) $ab \equiv a'b' \bmod n$.

Proof: Since $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$, the number n divides $a - a'$ and $b - b'$, i.e., $a - a' = kn$ and $b - b' = \ell n$, where $k, \ell \in \mathbb{Z}$. Then n also divides

$$(a+b)-(a'+b') = (a-a')+(b-b') = kn+\ell n = (k+\ell)n,$$

$$(a-b)-(a'-b') = (a-a')-(b-b') = kn-\ell n = (k-\ell)n,$$

$$\begin{aligned} ab - a'b' &= ab - ab' + ab' - a'b' = a(b-b')+(a-a')b' \\ &= a(\ell n) + (kn)b' = (a\ell + kb')n. \end{aligned}$$