NUMBER THEORY

ROBERT HOUGH

Theorem 1 (Fermat's little theorem)**.** *Let p be prime. Each non-zero $x \bmod p$ is a root of $x^{p-1} - 1 \equiv 0 \bmod p$.*

Proof. The non-zero elements of $\mathbb{Z}/p\mathbb{Z}$ form a multiplicative group. The order of any element of a group divides the order of the group. □

In fact, the group is cyclic. To see this, count the number of solutions to the equation $x^d - 1 \equiv 0 \bmod p$ for $d|(p-1)$. On one hand, since $\mathbb{Z}/p\mathbb{Z}$ is a field, the equation has at most d roots. On the other hand, $x^{\frac{p-1}{d}}$ is a root for each $x \not\equiv 0 \bmod p$, and the map $x \mapsto x^{\frac{p-1}{d}}$ is at most $\frac{p-1}{d}$ to 1, so there are at least d roots. Hence, by inclusion-exclusion, the number of generators of $(\mathbb{Z}/p\mathbb{Z})^\times$ is

$$\sum_{d|p-1} \mu\left(\frac{p-1}{d}\right) d = \phi(p-1) > 0.$$

Here $\phi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$ is the Euler phi function.

The *Hermite normal form* of an integer $m \times n$ matrix M is a factorization $M = UA$ where U is $m \times m$ integer matrix with determinant 1 or -1 and A is an integer matrix in row echelon form with non-negative integers in the pivots. To prove that the Hermite normal form exists, perform Gaussian elimination with the rows of the matrix, using the Euclidean algorithm to find integer combinations of the rows which eliminate the elements below the pivots.

Problem 1. Three infinite arithmetic progressions are given, whose terms are positive integers. Assuming that each of the numbers 1, 2, 3, 4, 5, 6, 7, 8 occurs in at least one of these progressions, show that 1980 necessarily occurs in one of them.

Problem 2. Prove that there is no infinite arithmetic progression whose terms are all perfect squares.

Problem 3. Prove that for no integer $n > 1$ does n divide $2^n - 1$.

Problem 4. For a positive integer n and a real number x, prove the identity

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \cdots + \left\lfloor x + \frac{n-1}{n} \right\rfloor = \lfloor nx \rfloor.$$

Problem 5. For p and q coprime positive integers prove the reciprocity law

$$\left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \cdots + \left\lfloor \frac{(q-1)p}{q} \right\rfloor = \left\lfloor \frac{q}{p} \right\rfloor + \cdots + \left\lfloor \frac{(p-1)q}{p} \right\rfloor.$$

Problem 6. Let n, a, b be positive integers. Prove that

$$\gcd(n^a - 1, n^b - 1) = n^{\gcd(a,b)} - 1.$$

Problem 7. Is it possible to place 1995 different positive integers around a circle so that for any two adjacent numbers, the ratio of the greater to the smaller is a prime?

Problem 8. Let p be a prime number. Prove that there are infinitely many multiples of p whose last ten digits are all distinct.

Problem 9. Find all positive integers n such that $n!$ ends in exactly 1000 zeros.

Problem 10. Let $(x_n)_n$ be a sequence of positive integers satisfying the recurrence relation $x_{n+1} = 5x_n - 6x_{n-1}$. Prove that infinitely many terms of the sequence are composite.

Problem 11. Let $f(x_1, ..., x_n)$ be a polynomial with integer coefficients of total degree less than n. Show that the number of ordered n-tuples $(x_1, x_2, ..., x_n)$ with $0 \leqslant x_i \leqslant 12$ such that $f(x_1, x_2, ..., x_n) \equiv 0 \bmod 13$ is divisible by 13.

Problem 12. Let p be an odd prime. Show that if the equation $x^2 \equiv a \bmod p$ has no solution then $a^{\frac{p-1}{2}} \equiv -1 \bmod p$.

Problem 13. A lattice point $(x, y) \in \mathbb{Z}^2$ is visible from the origin if x and y are coprime. Prove that for any positive integer n there exists a lattice point (a, b) whose distance from every visible point is greater than n.

Problem 14. Let α be a real number. Suppose that n^α is an integer for all positive integers n. Prove that α is a non-negative integer.

Problem 15. Let the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ act on the complex plane by fractional linear transformations,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}.$$

Prove that for every z with $\Im(z) > 0$ there is a matrix $M \in \mathrm{SL}_2(\mathbb{Z})$, the group of 2×2 integer matrices with determinant 1, such that $z' = M \cdot z$ satisfies $|\Re z'| \leqslant \frac{1}{2}$ and $|z'| \geqslant 1$.

Problem 16. Let a and b be positive integers. For a non-negative integer n let $s(n)$ be the number of non-negative integer solutions to the equation $ax + by = n$. Prove that the generating function of the sequence $(s(n))_n$ is

$$f(x) = \frac{1}{(1 - x^a)(1 - x^b)}.$$

Problem 17. Let p be a prime. Show that every integer matrix M of determinant p can be written as $M = UA$ where U is an integer matrix of determinant 1 and A is one of the following $p + 1$ matrices.

$$\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix},\ 0 \leqslant a < p.$$

These matrices are called 'Hecke points,' and play an important role in the theory of modular forms.

Problem 18. Given any vector $v \in \mathbb{Z}^n$, $n \geqslant 2$, the g.c.d. of whose entries is 1, prove that there is an integer matrix of determinant 1, the first column of which is v.

Problem 19. Let $p(x)$ be a polynomial of degree n with integer coefficients. If $M = \sup_{0 \leqslant x \leqslant 1} |p(x)|$, show that

$$M > \frac{1}{e^n}.$$