Discrete Math 37110 - Class 5 (2016-10-11)

Instructor: László Babai
Notes taken by Jacob Burroughs
Revised by instructor

5.1 Fermat's little Theorem

Theorem 5.1 (Fermat's little Theorem)**.** *If p is prime and* $\gcd(a,p) = 1$*, then* $a^{p-1} \equiv 1 \mod p$.

Equivalently, if p is prime then $(\forall a)(a^p \equiv a \mod p)$

DO 5.2. Prove that the two versions of FlT are indeed equivalent.

Example 5.3. We can show this simply for $p = 2, 3, 5$, noting that the product of k consecutive integers is always divisible by k.

$$\begin{aligned} a^2 &\equiv a \pmod 2 & 2 \mid a^2 - a &= a(a-1) \\ a^3 &\equiv a \pmod 3 & 2 \mid a^3 - a &= (a-1)a(a+1) \\ a^5 &\equiv a \pmod 5 & 5 \mid a^5 - a &= (a-1)a(a+1)(a^2+1) \\ & & &\equiv (a-1)a(a+1)(a^2-4) \\ & & &= (a-1)a(a+1)(a+2)(a-2) \end{aligned}$$

HW 5.4. Prove: if $a = 3k - 4$ and $b = 5k + 3$ then $\gcd(a, b) = 1$ or 29. **(7 points)**

Your proof sould take no more than two lines.

5.2 Infinitude of primes; primes in arithmetic progressions

Theorem 5.5 (Euclid: "Elements")**.** *There are infinitely many primes.*

Proof. Let us prove this by contradictions. Suppose $P = \prod_{i=1}^{m} p_i$ where $p_1, \ldots, p_m$ are all the primes. Let q be a prime divisor of $P + 1$, so $q \mid P + 1$. Since q is a prime, $(\exists j)(q = p_j)$. Therefore $q \mid P$, but we also have $q \mid P + 1$, so $q \mid 1$, a contradiction. □

XC 5.6. Prove: there exist infinitely many primes $p \equiv -1 \pmod 4$ **(6 points)**

XC 5.7. If p is prime and $p \mid 4a^2 + 1$ then $p \equiv 1 \pmod 4$. (Hint: Fermat's Little Theorem) **(5 points)**

XC 5.8. Use the preceding exercise to prove that there exist infinitely many primes $p \equiv 1 \pmod 4$. **(5 points)**

Theorem 5.9 (Dirichlet)**.**

$$(\forall a, b \geq 1)(\textit{if } \gcd(a,b) = 1 \textit{ then } \exists \textit{ infinitely many primes } p \equiv b \pmod{a})$$

The proof uses the theory of complex functions.

DO 5.10. If p is prime, $p \geq 5$, then $p \equiv \pm 1 \pmod 6$

DO 5.11. There exist infinitely many primes $p \equiv -1 \pmod 6$

CH 5.12. There exist infinitely many primes $p \equiv 1 \pmod 6$

5.3 Asymptotic equality; the Prime Number Theorem: Stirling's formula

Definition 5.13. We say $f \sim g$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$. For sequences $\{a_n\}$ and $\{b_n\}$ we say $a_n \sim b_n$ if $\lim_{n\to\infty} \frac{a_n}{b_n} = 1$.

Notation 5.14. Let $\pi(x)$ denote the number of primes $\leq x$.

Example 5.15.

$$\begin{aligned} \pi(10) &= 4 \\ \pi(100) &= 25 \\ \pi(2) &= 1 \\ \pi(\pi) &= 2 \\ \pi(-15) &= 0 \end{aligned}$$

Theorem 5.16 (Prime Number Theorem, Hadamard and de la Vallée Poussin, 1896)**.**

$$\pi(x) \sim \frac{x}{\ln x}$$

Probability that a random number from 1 to x is prime: $\frac{\pi(x)}{x} \sim \frac{1}{\ln x}$. We note that this goes to zero fairly slowly, so primes are relatively frequent.

Hilarious reading (not relevant to the course) by George Mikes: "How to be Alien."

Theorem 5.17 (Stirling's Formula)**.**

$$n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$$

We denote the set$\{1, \ldots, n\}$ by $[n]$. Now $n!$ is the number of permutations of $[n]$

Definition 5.18. A permutation of a set A is a bijection $A \to A$

5.4 Counting

Notation 5.19. Σ^n denotes the set of strings of length n over the finite alphabet Σ.

Example 5.20. Example: let $\Sigma = \{A, B, C\}$; then $ABBCA \in \Sigma^5$ and $|\{A, B, C\}^n| = 3^n$.

Definition 5.21. The set $\mathcal{P}(A)$ is the *powerset* of A: the set of all subsets of A.

Definition 5.22. Given $B \subset A$, the *indicator function* of B in A: $f_B : A \to \{0, 1\}$ is defined as follows: $f_B(x) = 1$ if $x \in B$ and $f_B(x) = 0$ if $x \in A \setminus B$. (This function indicates membership in B. It is also be called the *characteristic function* of B.)

Notation 5.23. Given A, B sets:

$$A^B = \{f : B \to A \text{ functions}\}$$

DO 5.24. $\left|A^B\right| = |A|^{|B|}$.

Hint. $\left|A^B\right|$ counts the strings of length $|B|$ over the alphabet A.

DO 5.25. The function $B \mapsto f_B$ is a bijection from $\mathcal{P}(A)$ to $\{0, 1\}^A$. This proves that $|\mathcal{P}(A)| = 2^{|A|}$.

HW 5.26 (Due Tuesday, 2016-10-18)**.** Count the $(0, 1)$ strings of length n without consecutive 1s. Express this in closed form (no summation or product) through a sequence we have already encountered. Prove your answer. **(7 points)**

Notation 5.27. We denote the number of k-subsets of an n-set by the symbol $\binom{n}{k}$ ("n choose k").

Theorem 5.28. *(a) For $0 \le k \le n$ we have $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.* *(b) If $k > n$ then $\binom{n}{k} = 0$.*

Statement (b) is obvious. We prove a generalization of statement (a).

Theorem 5.29 (Permutations with repeated entries)**.** *Let X be a string of n letters over the alphabet $\Sigma = \{A_1, \ldots, A_m\}$. Let k_i denote the multiplicity of of A_i (number of occurrences of A_i) in X. (So $k_i \ge 0$ and $\sum_{i=1}^m k_i = n$.) Then the number of permutations of X is $\dfrac{n!}{\prod(k_i!)}$.*

Proof. For notational convenience we describe the proof for the case $m = 3$ and alphabet $\Sigma = \{A, B, C\}$. The general case works the same way. Let us label the occurrences of A as $A_1, \ldots, A_{k_1}$, the occurrences of B as $B_1, \ldots, B_{k_2}$, etc. Now all letters are distinct, so there are $n!$ permutations. Let us now drop the labels; let us say that two labeled strings are equivalent if their unlabeled versions are equal. So for instance, $A_2A_3B_2A_1B_1$ is equivalent to $A_1A_3B_1A_2B_2$ since when we unlabel them, both will become the string $AABAB$. This is an equivalence relation of labeled strings; what we need to count is the equivalence classes. Each equivalence class consists of $\prod k_i!$ permutations, so the number of equivalence classes is $\dfrac{n!}{\prod(k_i!)}$. □

Remark 5.30. The instructor calls the method used "King Matthias's shepherd's method." (The shepherd counted his sheep by counting their legs and dividing by 4, noting that there was a natural equivalence relation on legs ("belongs to the same sheep") and each equivalence class has size 4.)

DO 5.31. Derive part (a) of Theorem 5.28 from Theorem 5.29. Hint: Use the alphabet $\Sigma = \{0, 1\}$ (so $m = 2$) and encode each k-subset by its indicator function viewed as a string of k 1s and $n - k$ 0s.

Theorem 5.32 (Binomial Theorem)**.**

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Proof. $(x_1 + y_1)(x_2 + y_2) \cdots (x_n + y_n) = \sum_{I \subseteq [n]} \prod_{i \in I} x_i \prod_{j \notin I} y_i$
After dropping subscripts, we get $\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ □

Theorem 5.33 (Trinomial Theorem)**.**

$$(x + y + z)^n = \sum_{k_1,k_2,k_3 \geq 0, k_1+k_2+k_3=n} \binom{n}{k_1, k_2, k_3} x^{k_1} y^{k_1} z^{k_1}$$

where $\binom{n}{k_1, k_2, k_3} = \dfrac{n!}{k_1! k_2! k_3!}$

DO 5.34. Multinomial theorem:

$$(x_1 + \cdots + x_r)^n = \sum_{k_i \geq 0, \sum k_i = n} \binom{n}{k_1, \ldots, k_r} x_1^{k_1} \cdots x_r^{k_r}$$

where $\binom{n}{k_1, \ldots, k_r} = \dfrac{n!}{\prod k_i!}$.

DO 5.35.

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}.$$

DO 5.36.

$$\binom{n}{3} \sim \frac{n^3}{6}.$$

HW 5.37. Express $\binom{2n}{n}$ asymptotically as $\binom{2n}{n} \sim a n^b c^n$. Find the constants a, b, c. **(6 points)**

DO 5.38. Find constants a and b such that

$$\sqrt{n^2 + 1} - n \sim a n^b$$

The number of terms in the binomial theorem is $n+1$. The number of terms in the trinomial theorem is $\binom{n+2}{2}$. The number of terms in the multinomial theorem is $\binom{n+r-1}{r-1}$.

DO 5.39. Prove the last statement above.

Hint. We need to count the solutions of the equation $k_1+\cdots+k_r = n$ in nonnegative integers k_i. Use the "stars and bars" method. (Look it up.)