Discrete Mathematics – CMSC-37110-1 Homework 9 – November 3, 2005

Instructor: László Babai Ry-164 e-mail: laci[at]cs[dot]uchicago[dot]edu

HOMEWORK. Please print your name on each sheet. Please try to make your solutions readable.

This homework is due next class, TUESDAY, NOVEMBER 8.

Please write solutions to challenge problems on a separate sheet.

READ: generating functions from Matoušek–Nešetřil text.

The DO problems are for practice, do not hand them in.

DO9.1 (a) Prove: $a - b \mid a^m - b^m$. (b) Prove: if m is odd then $a + b \mid a^m + b^m$.

DO9.2 (a) Prove: If $n \geq k \geq 2$ are integers then $\lfloor n/k \rfloor + \lfloor (n+1)/k \rfloor \leq \lfloor (2n)/k \rfloor$. (b) Use part (a) to infer that $n+1$ divides $\binom{2n}{n}$. (Hint. What you need to prove is that $n!(n+1)!$ divides $(2n)!$. For every prime p, compare the largest power of p dividing each of these two numbers.)

DO9.3 (a) Prove that 10 is a primitive root modulo 7 (see def in HW9.3). (b) Link this to the fact that the decimal expansion of $1/7$ is periodic and the length of the period is 6. (c) Prove that 10 is a primitive root modulo 17. (d) Link this to the fact that the decimal expansion of $1/17$ is periodic and the length of the period is 16. (e) For a prime $p \geq 7$, show that the deciaml expansion of $1/p$ is periodic with period of length $p-1$ if and only if 10 is a primitive root mod p.

DO9.4 (a) Prove: if $a^2 \equiv b^2 \pmod{p}$ where p is a prime then $a \equiv \pm b \pmod{p}$. (b) Use part (a) to prove that for a prime $p \geq 3$, exactly $(p-1)/2$ residue classes mod p consist of quadratic residues mod p. (For the definition of quadratic residues, see HW9.3.)

DO9.5 (a) Prove that the product of two quadratic residues is a quadratic residue. (b) Prove that the product of a quadratic and a quadratic nonresidue is a nonresidue. (An integer b is a quadratic nonresidue if $(\forall x)(x^2 \not\equiv b \pmod{p})$.) (c) Prove that the product of two quadratic nonresidues is a quadratic residue. (Hint. This is trickier than (a) or (b). You need to use parts (a), (b), and 9.2(b).)

DO9.6 Prove: the system of simultaneous congruences

$x \equiv a_1 \pmod{m_1}$ and

$x \equiv a_2 \pmod{m_2}$

has a solution if and only if $\gcd(m_1, m_2) \mid a_1 - a_2$.

DO9.7 Consider the sequence $1, 1, 1, \ldots$. Verify that (a) the ordinary generating function of the sequence is $\dfrac{1}{1-x}$; (b) the exponential generating function is e^x.

Homework (due at the beginning of class **Tuesday, Nov 8**):

HW9.1 (3+1 points) Recall that $\lfloor x \rfloor$, the "floor" of x is its rounded-down value, i. e., $\lfloor x \rfloor = k$ is the unique integer such that $k \leq x < k+1$. (a) Prove: $\lfloor x+y \rfloor - 1 \leq \lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x+y \rfloor$. (b) Infer from part (a) that $0 \leq \lfloor 2x \rfloor - 2\lfloor x \rfloor \leq 1$.

HW9.2 (4 points) As in class, let $k_p(n)$ denote the largest integer such that $p^{k_p(n)}$ divides $n!$ (where p is a prime and $n \geq 1$). Prove: $k_p(n) < n/(p-1)$.

HW9.3 (4 points) Recall that a number a is a **quadratic residue** mod p if $x \not\equiv 0 \pmod p$ and $(\exists x)(x^2 \equiv a \pmod p)$. Example: the quadratic residues mod 13 are the residue classes represented by $1, 4, 9, 16, 25, 36$, i. e., the residue classes represented by $1, 3, 4, 9, 12, 10$. Recall further that a number g is a **primitive root** mod p if g^{p-1} is the smallest power of g congruent to 1 mod p. In other words, $g, g^2, \ldots, g^{p-1}$ are pairwise incongruent mod p and therefore they form a reduced set of residues mod p. Prove: (a) for an odd prime p, a quadratic residue mod p is never a primitive root. (b) (Challenge problem) Prove: The number of primitive roots mod p is $\varphi(p-1)$ where φ denotes Euler's phi function. (c) (Challenge problem) If p is a Fermat prime, i. e., a prime of the form $p = 2^{2^n} + 1$ (see HW9.6), then every quadratic nonresidue is a primitive root mod p.

HW9.4 (4+4 points) The DISCRETE LOGARITHM PROBLEM takes the numbers g, a, p as inputs (where p is a prime, g is a primitive root mod p, and $\gcd(a, p) = 1$), and asks to compute an exponent x such that $g^x \equiv a \pmod p$. (a) Show, with as little computation as possible, that $g = 2$ is a primitive root modulo $p = 13$. Show all your work. (b) Solve the following discrete logarithm problem by inspection: $2^x \equiv 7 \pmod{13}$. Verify your answer. Show all steps.

HW9.5 (3+4 points) (a) Prove: if $n > 0$ and $n \equiv -1 \pmod 4$ then n has a prime divisor p such that $p \equiv -1 \pmod 4$. (b) Use the result of (a) to demonstrate the infinitude of the primes $p \equiv -1 \pmod 4$.

HW9.6 (5+5 points) (a) Prove: If $2^k - 1$ is a prime then k must be a prime. (Hint: use the fact that $a - b \,|\, a^m - b^m$.) (Note: Not all numbers of the form $2^p - 1$ are prime: $2^{11} - 1 = 23 \cdot 89$. Primes of the form $2^p - 1$ are called *Mersenne primes.* At every point in recorded history, the largest known prime number was a Mersenne prime (see the Guinness Book of World Records). It is conjectured that there are infinitely many Mersenne primes. (b) Prove: If $2^k + 1$ is a prime then k itself is a power of 2. (Hint: use that if m is odd then $a + b \,|\, a^m + b^m$.) (Note: not all numbers of the form $2^{2^n} + 1$ are prime. Primes of this form are called *Fermat primes.* The only known Fermat primes are $3 = 2^{2^0} + 1, 5 = 2^{2^1} + 1$, $17 = 2^{2^2} + 1$, $257 = 2^{2^3} + 1$, $65,537 = 2^{2^4} + 1$. It is known (Euler) that $2^{2^5} + 1$ is composite. It is conjectured that there are only finitely many Fermat primes; possibly only those listed here. In one of the first striking applications of complex numbers, Gauss proved in his dissertation that a regular p-gon (p prime) can be constructed by a straightedge and a compass if and only if p is a Fermat prime, and he gave an explicit construction for $p = 17$. His grave was adorned by a 17-gonal gravestone.)

HW9.7 (a:2+5; b:4+5) Find simple closed-form expressions for (a) the ordinary and (b) the exponential generating functions of the following sequences: (1) $1, 0, 1, 0, \ldots$; (2) $0, 1, 2, 3, \ldots$.

HW9.8 (Challenge problem) **(Euler)** (a) Prove: $\sum_p 1/p = \infty$. Hint: refine Euler's proof of the infinitude of primes, discussed in class. (b) With further refinement, prove: there exists a constant c such that $\sum_{p \le x} 1/p = \ln\ln x + c + o(1)$. In other words, the quantity $\sum_{p \le x} 1/p - \ln\ln x$ approaches a finite limit as $x \to \infty$.

HW9.9 (Challenge problem) Determine the probability that two random positive integers are relatively prime. Use Euler's formula: $\sum_{i=1}^{\infty} 1/i^2 = \pi^2/6$. - For the question to make sense, we need to define what we mean by "random integers." Uniform distribution does not exist over a countable set. Let p_n be the probability that a pair of integers chosen uniformly from

$\{1, \ldots, n\}$ is relatively prime. Let $p = \lim_{n\to\infty} p_n$. The question is to determine p. It is not evident, and it is somewhat tedious to prove that this limit exists. The beauty of the problem is that assuming that this limit exists, one can prove in just a couple of lines that $p = 6/\pi^2$. Do this (compute the limit assuming it exists).