15-750 Algorithms (Spring 2002) **Prof. Manuel Blum**

Homework #9 **Solutions**

Problem 1: Wilson & Fermat (10 points)

(parts (b) and (c) of this problem are from "Concrete Mathematics" by Graham, Knuth & Patashnik)

Wilson's Theorem says that if p is prime then $(p-1)! \equiv -1(\mod p)$.

(a) prove Wilson's theorem

(b) show that if $p \mod 4 = 3$, then there is no integer n such that p divides n^2+1

(c) show that if $p \mod 4 = 1$, then there is such an integer n. (i.e. such that p divides n^2+1)

Hint: Think about Wilson's Theorem and Fermat's Little Theorem

(a) If $p=2$ the theorem is clearly true. If $p>2$, then the product $(p-1)!$ contains all the elements from $\mathbb{Z}_p^*$, so we can pair each element with it's inverse. The only elements in $\mathbb{Z}_p^*$, which are their own inverses $\mod p$, are 1 and -1. Hence $(p-1)! = 1(p-1) = -1 \mod p$. □

(b) Let $p = 4k+3$ and assume there exists n such that p divides n^2+1. This means, that $n^2 = -1 \mod p$. Clearly, $\gcd(n,p) = 1$, so by Fermat's Little Theorem, $n^{p-1} = 1 \mod p$. But $n^{p-1} = (n^2)^{2k+1} = (-1)^{2k+1} = -1 \mod p$, hence contradiction. □

(c) Let $p = 4k+1$ and consider $n = (2k)! \mod p$. We have

$$\begin{aligned} n^2 &= 1 \cdot 1 \cdot 2 \cdot 2 \cdot \ldots \cdot 2k \cdot 2k \mod p \\ &= (-1)^{2k} 1 \cdot (-1) \cdot 2 \cdot (-2) \cdot \ldots \cdot 2k \cdot (-2k) \mod p \\ &= (-1)^{2k}(p-1)! \mod p \\ &\overset{\text{Wilson}}{=} -1 \mod p\,. \end{aligned}$$

□

Problem 2: Funny primes (10 points)

(this problem is from "Concrete Mathematics" by Graham, Knuth & Patashnik)

The number 1111111111111111111 is prime. Prove that, in any positive integer base b, the number $(\underbrace{11111\ldots1}_{n\ 1's})_b$ can be prime only if n (the number of 1's) is prime.

Assume that $N = (\underbrace{11111\ldots1}_{n\ 1's})_b$ is prime and $n = r \cdot s$, $r, s \neq 1$. Then can easily verify that

$$(b^0 + b^1 + \ldots + b^{r-1}) \cdot (b^0 + b^r + b^{2r} + \ldots + b^{(s-1)r}) = b^0 + b^1 + \ldots + b^{rs-1} = N\,,$$

hence contradiction. □

Problem 3: Darts and permutations (15 points)

Show that the dartboard method works correctly to generate a random permutation on n letters.

Recall that the dartboard method for generating permutations works as follows: when a dart cuts off a segment of length ℓ, a random cycle of length ℓ is selected (i.e. we pick at random a subset of ℓ letters and put them into a random order, which defines the cycle), and the process is repeated on the remaining portion of the dartboard, with the remaining letters.

Consider any permutation π on n elements, where π consists of k cycles $c_1, \ldots, c_k$. We will prove that the dartboard method generates permutation π exactly with probability $1/n!$.

The proof is induction on k. Let $P_{n,k}$ denote the probability that the dartboard method generates a particular n-element permutation with k cycles, $\pi = c_1, c_2 \ldots, c_k$. Let ℓ_i denote the length of cycle c_i.

Base case: If $k = 1$, then with probability $1/n$ we hit the rightmost slot, and then with probability $1/(n-1)!$ we choose the correct cycle, which yields in total $1/n!$.

Induction step: Since any of the cycles in *pi* can be generated as the first one, we get

$$\begin{aligned} P_{n,k} &= \sum_{i=1}^{k} \frac{1}{n} \cdot \frac{1}{\binom{n}{\ell_i}(\ell_i - 1)!} \cdot P_{n-\ell_i,k-1} \\ &= \sum_{i=1}^{k} \frac{(\ell_i)!(n-\ell_i)!}{n\,n!(\ell_i-1)!} \cdot P_{n-\ell_i,k-1} \\ &\overset{\text{ind. hyp.}}{=} \frac{1}{n!} \sum_{i=1}^{k} \frac{\ell_i (n-\ell_i)!}{n} \cdot \frac{1}{(n-\ell_i)!} \\ &= \frac{1}{n!} \sum_{i=1}^{k} \frac{\ell_i}{n} = \frac{1}{n!} . \end{aligned}$$

□

Problem 4: Let's play darts (15 points)

Use the dartboard method to compute the following:

(a) probability that a randomly chosen n-bit number is a product of exactly two primes (not necessarily of equal lengths).

(b) probability that a randomly chosen n-bit number is divisible by at least one prime of length at least $n/2$ (assuming that n is even).

As in the lecture, a "bit" in this problem is taken to base e. The probabilities should be given in a closed form, or as asymptotic limits, not as recursive formulas.

(a) The generated number will be a product of exactly two prime numbers only if the first dart hits any slot except the last one (i.e. the rightmost one), and the second dart hits the last slot.

Hence the desired probability P is

$$
\begin{aligned}
P &= \sum_{i=1}^{n-1} \frac{1}{n} \cdot \frac{1}{n-i} \\
&= \frac{1}{n} \sum_{i=1}^{n-1} \frac{1}{n-i} \\
&= \frac{H_{n-1}}{n} \longrightarrow \frac{\ln n}{n} ,
\end{aligned}
$$

where H_n denotes n-th harmonic number.

(b) Let $P_{n,k}$ denote the probability that a randomly chosen n-bit number is divisible by at least one prime of length at least k. We are interested in $P_{2k,k}$.

Clearly, $P_{k,k} = 1/k$, and $P_{m,k} = 0$ for $m < k$. Further we get

$$
\begin{aligned}
P_{k+1,k} &= \frac{2}{k+1} + \frac{1}{k+1} P_{k,k} = \frac{1}{k} + \frac{1}{k+1} \\
P_{k+2,k} &= \frac{3}{k+2} + \frac{1}{k+2} (P_{k+1,k} + P_{k,k}) = \frac{1}{k} + \frac{1}{k+1} + \frac{1}{k+2} ,
\end{aligned}
$$

and generally for any integer c, $1 \le c \le k$

$$
P_{k+c,k} = \frac{1}{k} + \frac{1}{k+1} + \ldots + \frac{1}{k+c} = H_{k+c} - H_{k-1} .
$$

Therefore

$$
P_{n,n/2} = H_n - H_{n/2-1} \longrightarrow \ln(n) - \ln(n/2) = \ln 2 \approx 0.693 .
$$