Homework 5

CSE/MATH 467 Due: 23 September, 2016

1. (Coding problem from last week) Write fast exponentiation code and find ten 10-digit probable primes (with respect to base 2).

2. a) Determine $13^{13^{13}}\%10$.
b) Determine $13^{13^{13}}\%15$.

3. Recall that we formulated Garner's fast recursive general Chinese Remainder Theorem in the following way:
Input:
Moduli $m_1, \ldots, m_r$ with $\gcd(m_i, m_j) = 1$ when $i < j$.
Representatives $a_1, \ldots, a_r \in \mathbb{Z}$
Algorithm: Define recursively A_k (kth interpolation) and w_k (kth weight) by the following:
Intialization:

- $w_1 := 0$.
- $w_1 := A_1 := a_1\%m_1$.

Recursion:

- $w_{k+1} := (a_{k+1} - A_k)(m_1 \cdots m_k)^*\%m_{k+1}$
- $A_{k+1} := A_k + (w_{k+1}m_1 \cdots m_k)$,

where $(m_1 \cdots m_k)(m_1 \cdots m_k)^* \equiv 1 \mod m_{k+1}$.

A. Show by induction on r that $A_r = w_1 + w_2m_1 + \cdots + w_rm_1 \ldots m_{r-1}$ satisfies the system of congruences

$$x \equiv a_1 \mod m_1$$
$$\vdots$$
$$x \equiv a_r \mod m_r$$

B. At most how many multiplications modulo m_k are actually involved in the kth step if we take care to keep the sizes of numbers down? (Ignore those coming from multiprecision considerations and from the Knuth algorithm to compute multiplicative inverses modulo m_k.)

4. Let p and q be odd primes with difference $\delta = p - q > 0$ and product $n = pq$.

(a) Show that the Fermat factorization method involves $(p+q)/2 - \lceil\sqrt{n}\rceil$ increases in x to find x and y such that $n = x^2 - y^2$.

(b) Show that

$$\left(\frac{p+q}{2} - \sqrt{pq}\right)\left(\frac{p+q}{2} + \sqrt{pq}\right) = \frac{1}{4}\delta^2.$$

(c) Assume that δ is so much smaller than p that we can consider $(p+q)/2 \approx p$ and $\sqrt{pq} \approx p$. Show that then

$$\left(\frac{p+q}{2} - \sqrt{pq}\right) \approx \frac{\delta^2}{8p}.$$

(d) Suppose that p and q are 100-digit primes (so that $p, q \approx 10^{99}$) and $p - q \approx 10^{80}$ so the most significant 19 or 20 digits are the same. Show that the Fermat algorithm takes approximately 10^{60} increases in x.

(e) If p and q are 100-digit primes with $p - q \approx 10^{50}$, show that the Fermat method finds the factorization with very few increases in x.

5. We showed in class that if $m, n \in \mathbb{N}$ are relatively prime, then $\phi(mn) = \phi(m)\phi(n)$. Prove by *careful induction* that if $m_1, \ldots, m_r$ are pair-wise relatively prime positive integers, then $\phi(m_1 \cdot m_r) = \phi(m_1)\cdots\phi(m_r)$. You may take $r = 2$ as the base case.