Notes on Agrawal, Kayal and Saxena's Primes in P

Burton Rosenberg

April 7, 2003

The algorithm

```
Initial step: if n is a^b, b>1, return composite
While loop:
     Find a prime r such that q, the largest prime factor of r-1 satisfies:
     1) q>=4 Sqrt[r] log n
     2) n^((r-1)/q) != 1 (mod r)
     If find a factor of n in while loop ( gcd(n,r)!=1) return composite
For loop:
     For a=1,...,2 Sqrt[r] log n, check.
     1) gcd(a,n)=1
     2) (x-a)^n = (x^n-a) (mod x^r-1,n)
     If ever fails, return composite
Return prime
```

Regarding initial step of algorithm

Lemma 1 (Detecting pure powers) *There is a polynomial time algorithm for deciding if n is of the form m^j, where n, m, j are integers.*

Proof: Suppose $n = m^j$, with j a positive integer and m a real. Then,

$$j = \frac{\log_2 n}{\log_2 m} \leq \log_2 n.$$

Attempt the integer j-th root of n for $j = 2, \ldots, \lfloor \log_2 n \rfloor$. The j-th root of n can be determined by binary search for the m between 1 and n such that $m^j = n$. The process is $O(\log^k n)$ for some integer k. □

Regarding while loop of algorithm

There are two items at issue here. First is the finding of a prime r for which prime q, $q \,|\, (r-1)$, is large, the second item is to get that $q \,|\, o_r(n)$, where $o_r(n)$ is the order of n mod r. We use the facts,

Lemma 2 (Density of Primes) *Let $\pi(x)$ be the number of primes less than or equal to x. For $x \geq 1$,*

$$\frac{x}{6\log_2 x} \leq \pi(x) \leq \frac{8x}{\log_2 x}.$$

Lemma 3 (Density of Special Primes) *Let $P(n)$ denote the greatest prime divisor of n. Exists $c > 0$ and n_o such that for all $n \geq n_o$,*

$$|\{\, p \leq x \,|\; p \text{ prime and } P(p-1) > x^{2/3} \,\}| \geq c\frac{x}{\log_2 x}.$$

Such primes are called *special*.

Lemma 4 (Existence of a special prime) *Exists c_1, c_2, c_3 such that there is a prime r,*

$$c_1 \log^6 n \leq r \;\; \leq c_2 \log^6 n$$

such that $r-1$ has a prime factor $q \geq 4\sqrt{r}\log_2 n$. In fact, the number of such primes is $c_3 \log^6 n / \log\log n$.

Proof: First count the number of primes r in the given interval which have large enough divisors of $r-1$. Since large enough will be $r^{2/3}$, and also greater than $4\sqrt{r}\log_2 n$, we will need to consider large enough r as well.

$$\begin{aligned}
b &= (\text{number of special primes} < c_2 \log^6 n) - (\text{number of primes} < c_1 \log^6 n\ ) \\
&\geq \frac{cc_2 \log_2^6 n}{\log_2(c_2 \log_2^6 n)} - \frac{8c_1 \log^6 n}{\log_2(c_1 \log^6 n)} \\
&\geq \left(\frac{cc_2}{7} - \frac{8c_1}{6}\right) \frac{\log_2^6 n}{\log\log_2 n}.
\end{aligned}$$

Chose $c_1 \geq 4^6$ and then choose c_2 so that the above bound is positive, say c_3. For this r,

$$q > r^{2/3} = \sqrt{r} r^{1/6} \geq \sqrt{r}(c_1 \log_2^6 n)^{1/6} \geq 4\sqrt{r}\log_2 n.$$

□

We now pick from the special primes those for which the large prime factor q of $r-1$ divides $o_r(n)$.

Lemma 5 (Detecting q divides $o_r(n)$) *Let r and q be primes, and $q \,|\, r-1$. Let $o_r(n)$ be the order of n in F_r. Then $n^{(r-1)/q} \neq 1 \bmod r$ implies $q \,|\, o_r(n)$.*

Proof: Since $o_r(n) \,|\, r-1$,

$$n^{r-1} = n^{o_r(n)k} = 1 \bmod n$$

for some integer k. If $q \not| o_r(n)$ then $q \,|\, k$ and,

$$n^{(r-1)/q} = n^{o_r(n)(k/q)} = 1 \bmod n$$

□

Lemma 6 *There are at most $\lfloor \log_2(n) \rfloor$ prime factors in n.*

Proof: Denote by k the number of prime factors. Let $n = \Pi p_i^{e_i}$ be the prime decomposition of n. Then

$$\log_2 n = \sum e_i \log_2 p_i \geq \sum e_i \geq k.$$

□

Lemma 7 *There are at most $x^{2/3} \log_2 n$ prime factors in the product $\pi = (n-1)(n^2-1)\ldots(n^{x^{1/3}} - 1)$.*

Proof: We upper bound the size of π and take the log.

$$\pi = \prod_{i=1}^{x^{1/3}} (n^i - 1) \leq \prod n^i = n^{\sum i} \leq n^{x^{2/3}}$$

□

Lemma 8 *Among the special primes the Special prime lemma, there are r such that the q dividing $(r-1)$ also divides $o_r(n)$.*

Proof: Consider the product π from the previous lemma with $x = c_2 \log_2^6 n$. Then,

$$x^{2/3} \log_2 n = (c_2)^{2/3} \log_2^5 n < \frac{c_3 \log_2^6 n}{\log \log_2 n}$$

Hence there must be some special prime r which is not among the prime factors of π. For this r, $o_r(n) > (c_2 \log_2^6 n)^{1/3} > r^{1/3}$. Since $o_r(n)|(r-1)$, the order must include enough large factors of $r-1$, but $(r-1)/q \leq r^{1/3}$, so $q|o_r(n)$. □

Regarding for loop of algorithm

Let $l = 2\sqrt{r}\log_2 n$. We investigate the consequence of,

$$(x-a)^n = (x^n - a) \bmod (x^r - 1, n), \ \forall a = 1, 2, \ldots, l.$$

We first establish a fact about what could be called the cyclotomic extension of F_p.

Lemma 9 *Suppose $h(x)$ is a factor of $x^r - 1$, r prime, and $m_1 = m_2 \bmod r$. Then $x^{m_1} = x^{m_2} \bmod h(x)$.*

Proof: Since $x^r = 1 \bmod h(x)$, then,

$$x^{m_1 - m_2} = x^{rt} = 1 \bmod h(x).$$

so $x^{m_1} = x^{m_2} \bmod h(x)$. □

Lemma 10 (Degree of a cyclotomic extension) *Let p and r be distinct primes and $o_r(p)$ the order of p in F_r. The irreducible factors of $(x^r - 1)/(x-1)$ in F_p are all of degree $o_r(p)$.*

Proof: Let $h(x)$ be an irreducible factor of $(x^r - 1)/(x-1)$. Working in $F_p[x]/h(x) = GF(p^k)$ some k, $g(x^p) = g(x)^p$, so $g(x^{p^d}) = g(x)^{p^d}$. Let $d = o_r(p)$, so that $p^d = 1 \bmod r$. By the mod r lemma, $g(x) = g(x)^{p^d}$. So $g(x)^{p^d - 1} = 1$. Thus $(p^k - 1) \,|\, (p^d - 1)$, implying $k \,|\, d$ (consider formal division).

Also, $h(x) \,|\, (x^r - 1)$ implies $x^r = 1 \bmod h(x)$. Since r is prime, the order of x in $F_p[x]/h(x)$ is r so $r \,|\, (p^k - 1)$, the order of the group. But $d = o_r(p)$, so $d \,|\, k$. We conclude that $k = d$. □

Lemma 11 *Let the prime factors of n be p_i. Since $q|o_r(n)$, then among the the p_i there is a prime factor p such that $q \,|\, o_r(p)$, where q is the largest prime factor of $r-1$.*

Proof: If $p_i^t = 1 \bmod r$ for all i, then $n^t = 1 \bmod r$. Hence $o_r(n) | \mathrm{lcm}\{o_r(p_i)\}$. Since q is prime and $q|o_r(n)$, there must be some p_i, say p, such that $q|o_r(p)$. □

Guidance: We can consider the situation $F_p[x]/h(x) = \mathrm{GF}(p^d)$, where the irreducible factor $h(x)$ of $x^r - 1$ is of degree $d = o_r(p)$. Since $p|n$ and $h(x)|(x^r - 1)$, the tested congruences hold in $F_p[x]/h(x)$. The jist of the for loop is that if the congruences under consideration hold, then $n = p^k$, some k. We look at the group generated by the binomials which have been verified, and define a certain set based on the generator for that group.

Lemma 12 (Group of checked polynomials) *In the field $F_p[x]/h(x)$, where p is a prime dividing n and $h(x)$ is an irreducible factor of $x^r - 1$ of degree $d = o_r(p)$, consider the set G of polynomials generated by binomials $(x-a)$, where $1 \le a \le l$. This is a cyclic subgroup of $(F_p[x]/h(x))^*$ of degree greater than $n^{2\sqrt{r}}$.*

Proof: As a subgroup of a finite cyclic group, it is cyclic. We have verified that all the constants are coprime to p. For generated polynomials of degree less than d, no two will be congruent mod $h(x)$. This gives $\binom{l+d-1}{l}$ distinct polynomials. We have a bound on d since $q|d$, and $q \geq 4\sqrt{r}\log_2 n$, and $l = 2\sqrt{r}\log_2 n$,

$$\binom{l+d-1}{l} > \left(\frac{d}{l}\right)^l \geq \left(\frac{q}{l}\right)^l \geq 2^l = n^{2\sqrt{r}}.$$

□

Definition 1 *Let $g(x)$ be a generator for the cyclic group G. Define,*

$$I_g = \{\, m \in \mathbf{Z} \,|\, g(x^m) = g(x)^m \bmod (x^r - 1, p) \,\}$$

Lemma 13 $p, n \in I_g$

Proof: Since $(x-a)^n = x^n - a \bmod (x^r - 1, p)$ has been verified for all generators of G, it is true for any element of G including g. Since the ground field F_p has characteristic p, $g(x)^p = g(x^p)$. □

Lemma 14 *The set I_g is closed under multiplication.*

Lemma 15 *Denote by o_g the order of $g(x)$ in $F_p[x]/h(x)$. Suppose $m_1, m_2 \in I_g$ and $m_1 = m_2 \bmod r$. Then $m_1 = m_2 \bmod o_g$.*

Proof: In $F_p[x]/h(x)$,

$$g(x)^{m_1} = g(x^{m_1}) = g(x^{m_2}) = g(x)^{m_2}$$

Hence $g(x)^{m_1 - m_2} = 1$, therefore $o_g \,|\, m_1 - m_2$. □

Theorem 16 *If the $l = 2\sqrt{r}\log_2 n$ congruences $(x-a)^n = (x^n - a) \bmod (x^r - 1, p)$ hold, then $n = p^j$, some j.*

Proof: Consider the set,

$$E = \{\, n^i p^j \,|\, 0 \leq i, j, \leq \sqrt{r} \,\}$$

By the multiplicative closure of I_g, $E \subseteq I_g$. There are $(1 + \lfloor\sqrt{r}\rfloor)^2 > r$ elements in this set, and therefore two are equal mod r. Hence two elements are equal mod o_g. Since $o_g = |G| > n^{2\sqrt{r}}$ and $n^{|i_1 - i_2|}, n^{|j_1 - j_2|} < n^{\sqrt{r}}$, the congruence is an equality, that is, $n^{i'} = p^{j'}$. □