Summer School - Number Theory for Cryptography

F. Morain

Tutorial, 2013/06/25

1. Implement the AMR test.

2. Find a (probable) family of composite integers N satisfying $F(N) = \varphi(N)/4$.

Answer. This is taken from a paper by Beauchemin, Brassard, Crpeau and Goutier at CRYPTO'86.

Let us decide to find a family of numbers with two prime factors only. Write $N = p_1 p_2$ with $p_1 = 2^{s_1} t_1 + 1$, $p_2 = 2^{s_2} t_2 + 1$ with $1 \leq s_1 \leq s_2$. Note that $\varphi(N) = 2^{s_1+s_2} t_1 t_2$. Monier's formula gives us

$$F(N) = \left[1 + \frac{2^{2s_1} - 1}{2^2 - 1}\right] T_1 T_2$$

with $T_i = \gcd(p_i - 1, N - 1)$. We decide to try to have maximal odd part for $T_1 T_2$ by forcing $T_i = t_i$, which means that $t_i \mid N - 1$. But

$$N - 1 = (1 + 2^{s_1} t_1)(1 + 2^{s_2} t_2) - 1 = 2^{s_2} t_2 + 2^{s_1} t_1 + 2^{s_1+s_2} t_1 t_2.$$

The only possibility for $t_1 \mid N - 1$ is to have $t_1 \mid t_2$. The same being true for t_2, we must have $t_1 = t_2$. Monier's formula now reads

$$F(N) = \left[1 + \frac{2^{2s_1} - 1}{2^2 - 1}\right] t_1 t_2 = \left[1 + \frac{2^{2s_1} - 1}{2^2 - 1}\right] \frac{\varphi(N)}{2^{s_1+s_2}}.$$

The last thing to do is solve

$$\left[1 + \frac{2^{2s_1} - 1}{2^2 - 1}\right] \frac{1}{2^{s_1+s_2}} = \frac{1}{4}$$

or

$$\left[1 + \frac{2^{2s_1} - 1}{3}\right] = 2^{s_1+s_2-2},$$

equivalently

$$2^{2s_1-1} + 1 = 3 \cdot 2^{s_1+s_2-3}.$$

If $s_1 > 1$, the left hand side is odd, which implies $s_1 + s_2 = 3$. Since $1 < s_1 \leq s_2$, this is impossible. Now, we have $s_1 = 1$ and this implies $s_2 = 2$, or the family $(2t + 1)(4t + 1)$ with both terms prime.

We need $\pm t + 1 \not\equiv 0 \bmod 3$, leading to $t \not\equiv \pm 1 \bmod 3$, or $3 \mid t$. Remembering that t should be odd, we get $t = 6m+3$, leading to $N = (12m+7)(24m+13)$ with both factors simultaneously prime. This is the heuristic part, since we cannot prove that there exists an infinite number of m's leading to simultaneous prime values. However, examples are easy to find : $(m, N) = (0, 7 \times 13)$, $(1, 19 \times 37)$, $(2, 31 \times 61)$; $m = 6, 11, 16 \ldots$.

It might be possible to prove this is the only possible family, with more work.

3. Prove Pocklington's theorem.

4. a) Implement the $N - 1$ and find proven primes of the form $2 \cdot k! + 1$.
b) Same question with the $N + 1$ test and the family $2 \cdot k! - 1$.

5. We consider the equation $k\varphi(N) = N - 1$ for integers k and N.
a) solve the equation when $k = 1$.
Answer. $\varphi(N) = N - 1$ is only possible for prime N's.

From now on, fix some $k > 1$.
b) Give elementary properties of N's satisfying the equation.
Answer. N is a Carmichael number, hence odd, squarefree and for all $p_i \mid N$, one has $p_j \not\equiv 1 \bmod p_i$. Moreover, N has at least three (distinct) prime factors.
c) Find non-trivial bounds on the number of prime divisors t of a solution N to the equation.
Answer. We already know that $t \geq 3$. Let us give some results already obtained by Lehmer in his 1932 paper. We will often use the easy property that

Lemma. $x \mapsto x/(x-1)$ is decreasing.

Prop. (Lehmer) If $3 \leq t \leq 6$, then $k = 2$.
Proof: write

$$k = \prod_{i=1}^{t} \frac{p_i}{p_i - 1} - \frac{1}{\varphi(N)}.$$

We have $N \geq 105$ and $\varphi(N) \geq 48$ so that $k < 3$. □

Prop. (Lehmer) If $k = 3$, then $t > 32$.
Proof: $(N, 3) = 1$ implies $p_1 \geq 5$. Then $N \geq 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$ and $\varphi(N) \geq 18247680$ and

$$3 = \prod_{i=1}^{t} \frac{p_i}{p_i - 1} - \frac{1}{\varphi(N)}$$

leading to

$$\prod_{i=1}^{t} \frac{p_i}{p_i - 1} \geq 3 + \frac{1}{18247680} > 3.000000054$$

leading to the result, since the first larger value has 3.013375475 for $p_{33} = 149$, the previous one having value 2.993151479.

Until today, no non-trivial solution is known. Some are known for $k\varphi(N) = N + 1$, as for some other $N - a$. Some further properties can be found in recent papers (key word: *Lehmer totient problem*). □

5. a) Implement the AKS algorithm and prove that 89 is prime.
   b) Implement Berrizbeitia's variant and find some proven primes.