MAT 421 Number Theory
Takehome Exam 3

Note: Read the test instructions in my email carefully and thoroughly before you begin your exam. Failure to follow the instructions could result in point reductions or no point on individual problems.

1. (20pts) Use the repeated squaring method to compute the least residue of 2^{340} modulo 341.

   Solution. $340 = (101010100)_2 = 256 + 64 + 16 + 4$. Let $a = 2$ and $n = 341$.

k	$a^k \mod n$
4	16
8	$16^2 = 256$
16	$256^2 = 65536 \equiv 64 \mod 341$
32	$64^2 = 4096 \equiv 4 \mod 341$
64	$4^2 = 16$
128	$16^2 = 256$
256	$256^2 = 65536 \equiv 64 \mod 341$

   Hence,

$$\begin{aligned} 2^{340} &= 2^{256+64+16+4} \\ &= 2^{256} \cdot 2^{64} \cdot 2^{16} \cdot 2^4 \\ &\equiv 64 \cdot 16 \cdot 64 \cdot 16 \mod 341 \\ &\equiv 1 \mod 341 \end{aligned}$$

2. (10 pts) Use the Fermat's little theorem to show that 91 is not a prime.

   Solution. $2^{90} \equiv 64 \mod 91$, so 91 is not a prime.

3. (10 pts) Use the Lucas-Lehmer test to determine if $M_{11} = 2^{11} - 1$ is a prime.

   Solution. Since $S_{10} \equiv 1736 \mod 2047$, $M_{11} = 2^{11} - 1 = 2047$ is not a prime. In fact, $2047 = 23 \cdot 89$.

4. (20 pts) Factor 91 by the Monte Carlo Method with $f(x) = x^2 - 1$ and $x_0 = 2$. For each k step, compare x_k only with x_j for which $j = 2^h - 1$ where k is an $(h+1)$-bit integer.

   Solution.

   $$\begin{aligned}
   &x_1 = f(2) = 3\\
   &x_2 = f(3) = 8,\ (x_2 - x_1, n) = (8-3, 91) = 1\\
   &x_3 = f(8) = 63,\ (x_3 - x_1, n) = (63-3, 91) = 1\\
   &x_4 = f(63) \equiv 55 \mod 91,\ (x_4 - x_3, n) = (55-63, 91) = 1\\
   &x_5 = f(55) \equiv 21 \mod 91,\ (x_5 - x_3, n) = (21-63, 91) = 7
   \end{aligned}$$

   Hence, $91 = 7 \cdot 13$.

5. (10 pts) Use Fermat factorization to factor 809009.

   Solution. We try $t = [\sqrt{809009}] + 1 = 900, 901, 902, \cdots$ until $s^2 = t^2 - n$ is a perfect square.

   $$\begin{aligned}
   &900^2 - 809009 = 991, \text{ not a perfect square}\\
   &901^2 - 809009 = 2797, \text{ not a perfect square}\\
   &902^2 - 809009 = 4595, \text{ not a perfect square}\\
   &903^2 - 809009 = 6400 = 80^2
   \end{aligned}$$

   Hence,

   $$\begin{aligned}
   809009 &= (t+s)(t-s)\\
   &= (903+80)(903-80)\\
   &= 983 \cdot 823
   \end{aligned}$$

6. (10 pts) Use generalized Fermat factorization to factor 17018759.

Solution. We try $t = [\sqrt{5n}]+1 = [\sqrt{5 \cdot 17018759}]+1 = 9225, 9226, \cdots$ until $s^2 = t^2 - 5 \cdot 1708759$ is a perfect square.

$$9225^2 - 5 \cdot 17018759 = 6830, \text{ not a perfect square}$$
$$9226^2 - 5 \cdot 17018759 = 25281 = 159^2$$

$(t+s, n) = (9226+159, 17018759) = 1877$ and hence $17018759 = 1877 \cdot 9067$.

7. (20 pts) Use Pépin's test to show that $F_4 = 2^{16} + 1$ is a prime.

Solution. $3^{\frac{F_4-1}{2}} = 3^{2^{15}} \equiv 65536 \mod 2^{16}+1 \equiv -1 \mod 2^{16}+1$. Hence, $F_4 = 2^{16}+1$ is a prime.