Solutions to Assignment 13

M1. Find the prime divisors of the following numbers using Fermat's method ($N + x^2 = y^2$).

a. 437.

First we compute $\sqrt{437}$ = 20.9. So we calculate $21^2 - 437 = 4 = 2^2$.

So,

$437 + 2^2 = 21^2 \Rightarrow 437 = 21^2 - 2^2 = (21 + 2) \bullet (21 - 2) = 23 \bullet 19$.

b.* 1081.

$\sqrt{1081}$ = 32.8, so we try y's $\geq$ 33. We find $35^2 - 1081 = 144 = 12^2$.

So,

$1081 + 12^2 = 35^2 \Rightarrow 1081 = 35^2 - 12^2 = (35 - 12) \bullet (35 + 12) = 23 \bullet 47$.

c.* 1961.

Following the same steps as above we obtain,

$1961 + 8^2 = 45^2 \Rightarrow 1961 = 45^2 - 8^2 = (45 - 8) \bullet (45 + 8) = 37 \bullet 53$.

M2. Find the prime divisors of the following numbers using Pollard's p – 1 method.

Recall to factor a number N using Pollards p – 1 method, we calculate the following:

m_j = l.c.m(1,2,…,j).

$X_j = 2^{m_j} \bmod N$.

F_j = gcd ($X_j - 1$, N).

a. 3223

j	m_j	X_j	F_j
2	2	4	1
3	6	64	1
4	12	873	1
5	60	1893	11

Thus, 11 divides 3223. 3223/11 = 293.

Thus, 3223 = 11 • 293.

b.* 3977

j	m_j	X_j	F_j
2	2	4	1
3	6	64	1
4	12	119	1
5	60	1477	41

Thus, 41 divides 3977. 3977/41 = 97.

Thus, 3977 = 41 • 97.

c.* 862577

j	m_j	X_j	F_j
2	2	4	1
3	6	64	1
4	12	4096	1
5	60	603823	1
6	60	603823	1
7	420	16993	1
8	840	661331	1
9	2520	495336	631

Thus, 631 divides 862577. 862577/631 = 367.

Thus, $862577 = 631 \cdot 367$.

M3.* Why does Pollard's p – 1 method perform so badly on 274181?

The p – 1 method is slow to factor N when the factors of N all have large prime power factors. Put another way, the p – 1 method runs up to calculating l.cm(2,3,4…,j) where j is the smallest of (for each prime p dividing N), the largest prime power factor of p – 1.

For $274181 = 487 \cdot 563$ we see:

$563 - 1 = 2 \cdot 281$ – note 281 is prime, and

$487 - 1 = 486 = 2 \cdot 243$ – note $243 = 3^5$ (a large prime power).