Factoring - a summary so far

Suppose that $n = pq$ for primes p and q. It is reasonably easy to factor n if

- the difference between p and q is small (Fermat)
- at least one of the primes is small (Pollard's ρ algorithm) or
- if $p - 1$ has only "small" prime factors (Pollard's $p - 1$ algorithm).

Factoring - the quadratic sieve

Recall

Lemma

If $x^2 \equiv y^2$ mod n and $x \not\equiv \pm y$ mod n then n is composite. Moreover, $\gcd(n, x+y)$ and $\gcd(n, x-y)$ are non-trivial factors of n.

- The quadratic sieve method uses this lemma to hunt for factors. We need some terminology:
- A finite set of primes $F = \{p_1, p_2, \ldots, p_\ell\}$ (possibly containing the number -1) is called a factor base.
- A number r is said to be smooth with respect to a factor base F and a number n if $r \equiv r'$ mod n where the factorization of r' uses only primes in the factor base F.

Factoring - the quadratic sieve, cont'd

- Suppose we have a set $U = \{r_1, r_2, \ldots, r_k\}$ such that r_i^2 is smooth and in fact

$$r_i^2 \equiv p_1^{e_{i1}} p_2^{e_{i2}} \ldots p_\ell^{e_{i\ell}} \mod n$$

for each i. Moreover for each j

$$e_{1j} + e_{2j} + \ldots + e_{kj} = 2s_j.$$

- That is, the sum of the exponents for any given prime p_j in the factor set is even.
- Then we can let

$$x = \prod_{i=1}^{k} r_i \text{ and } y = \prod_{j=1}^{\ell} p_j^{s_j}.$$

- Then $x^2 \equiv y^2 \mod n$ and as long as $x \not\equiv \pm y \mod n$ then we find factors of n i.e. $\gcd(x + y, n)$ and $\gcd(x - y, n)$.

Factoring - the quadratic sieve, cont'd

- There are many questions about how to find F and U to satisfy all these conditions but first let's see a couple of examples.
- Starting small: $n = 4633$, $F = \{-1, 2, 3\}$ and $U = \{67, 68\}$.

$$67^2 \equiv -144 \equiv -2^4 \cdot 3^2 \text{ and } 68^2 \equiv -9 \equiv -3^2$$

mod 4633.

- Hence we have

$$(67 \cdot 68)^2 = 4556^2 \equiv (2^2 \cdot 3^2)^2 = 36^2 \bmod 4633$$

and $4556 \not\equiv \pm 36 \bmod 4633$ and so $\gcd(4592, 4633) = 41$ and $\gcd(4520, 4633) = 113$ divides 4633. In fact, $4633 = 41 \times 113$.

Factoring - the quadratic sieve, cont'd

- Where did U come from? As you can guess, once you decide on what U is you can decide on what F is once you start factoring.
- The hint here is that $\sqrt{4633} = 68.066\ldots$. If $x \approx \sqrt{n}$ then x^2 will be relatively small modulo n. Its factors will then also be small. We can allow a little liberty and consider $x \approx \sqrt{mn}$ for small m and then again, x^2 will be small modulo n and won't have large factors.
- In the first case, we used roughly $\sqrt{4633} \approx 68$ and $\sqrt{4633} - 1 \approx 67$. Notation: $[y]$ is the greatest integer less than or equal to y. So $[\sqrt{4633}] = 68$.
- Let's see a bigger example; this is the example in your book pgs. 183 - 185 but we will do it backwards.
- $n = 3837523$ and $[\sqrt{3837523}] = 1958$. We try numbers approximately of the size $[\sqrt{mn}]$ for various m's.

Factoring - the quadratic sieve, cont'd

- There are two ways to think about the factor set: you can either build it as you go i.e. factor each number that appears and add new factors to your factor set, or start with a smallish factor set and discard any number you generate that doesn't have those factors. I am not sure which your book did but let $F = \{2, 3, 5, 7, 11, 13, 17, 19\}$; all the primes less than 20.
- After much work with a computer, one obtains that the following numbers have squares which are smooth for n and F:

$$[\sqrt{n}] + 6, [\sqrt{3n}] + 4, [\sqrt{17n}] + 1, [\sqrt{23n}] + 4,$$
$$[\sqrt{53n}] + 1, [\sqrt{76n}] + 1 \text{ and } [\sqrt{95n}] + 2$$

which leads to the following congruences:

Factoring - the quadratic sieve, cont'd

$$
\begin{aligned}
1964^2 &\equiv 3^2 \cdot 13^3 \bmod n \\
3397^2 &\equiv 2^5 \cdot 5 \cdot 13^2 \bmod n \\
8077^2 &\equiv 2 \cdot 19 \bmod n \\
9398^2 &\equiv 5^5 \cdot 19 \bmod n \\
14262^2 &\equiv 5^2 \cdot 7^2 \cdot 13 \bmod n \\
17078^2 &\equiv 2^6 \cdot 3^2 \cdot 11 \bmod n \\
19095^2 &\equiv 2^2 \cdot 5 \cdot 11 \cdot 13 \cdot 19 \bmod n
\end{aligned}
$$

x^2	2	3	5	7	11	13	17	19
1964^2	0	0	0	0	0	1	0	0
3397^2	1	0	1	0	0	0	0	0
8077^2	1	0	0	0	0	0	0	1
9398^2	0	0	1	0	0	0	0	1
14262^2	0	0	0	0	0	1	0	0
17078^2	0	0	0	0	1	0	0	0
19095^2	0	0	1	0	1	1	0	1

Factoring - the quadratic sieve, cont'd

- In general you row-reduce this matrix modulo 2. The rows which correspond to all zeroes will indicate squares. The point is that since we are working with the exponents, addition will become multiplication and getting 0 mod 2 will mean that our exponents are even.
- With this matrix, we can eyeball the dependencies. Notice that 3 of the columns are all 0 so it is not hard to see that this matrix has rank 4 so we will get 3 usable equations.
- Row 1 + Row 5 = 0, Row 2 + Row 3 + Row 4 = 0 and Row 4 + Row 5 + Row 6 + Row 7 = 0 mod 2.

Factoring - the quadratic sieve, cont'd

This means that

$$\begin{aligned}(1964 \cdot 14262)^2 = 1147907^2 &\equiv 17745^2 = (3 \cdot 5 \cdot 7 \cdot 13^2)^2 \\ (3397 \cdot 8077 \cdot 9398)^2 &\equiv (2^3 \cdot 5^3 \cdot 13 \cdot 19)^2 \\ (9398 \cdot 14262 \cdot 17078 \cdot 19095)^2 &\equiv (2 \cdot 3 \cdot 5^4 \cdot 7 \cdot 11 \cdot 13 \cdot 19)^2\end{aligned}$$

all modulo n.

Using the basic principle, we get from the first equation that if $x = 1147907$ and $y = 17745$ we have $x \not\equiv \pm y \bmod 3837523$, hence the greatest common divisor of x - y = 1130162 and 3837523, which is 1093, gives a factor of 3837523. In fact 3837523 = $1093 \cdot 3511$.