Factoring - the quadratic sieve

- $n = 3837523$ and $[\sqrt{3837523}] = 1958$. We try numbers approximately of the size $[\sqrt{mn}]$ for various m's. 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

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

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 $x \not\equiv \pm y$ mod 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.

Discrete logarithms

- We are going to be interested in something called discrete logarithms. As you recall, with "real" logarithms, for real numbers a, b, c we say

$$log_a(b) = c \text{ iff } a^c = b.$$

  We want to generalize this to situations where we are treating objects a little more general than real numbers.
- Specifically, we want to make sense of

$$L_\alpha(\beta) = x \text{ iff } \alpha^x = \beta$$

  where x is an integer, α and β come from a finite field and the equality is equality in that field.
- The purpose for doing all this is that the ability to compute these so-called discrete logarithms is in principle hard and to carry out the exponentiations is relatively easy. We will build a cryptosystem called ElGamal based on these ideas.

Fields

- A field is a set F together with two binary operations $+$ and $\cdot$ which are both commutative and associative. Moreover, $+$ has an identity 0 and inverses for all elements; $\cdot$ has an identity 1 and inverses for non-zero elements and the two operations satisfy the distributive law:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

  for all a, b and c in F.
- You know many examples of fields: the real numbers with the usual addition and multiplication is a field; the complex numbers also with the usual $+$ and $\cdot$; the rational numbers (fractions) with the usual $+$ and $\cdot$. The integers is not a field since not every non-zero element has a multiplicative inverse (that's what the rationals are for!).

Finite fields

- You also know other examples of fields: Z_p for p a prime is a field. We saw that Z_n has a well-defined $+$ and $\cdot$ coming from the integers. If n is prime then we also know that if $ax \equiv 1 \mod n$ has a solution as long as $\gcd(a, n) = 1$ which happens as long as $a \neq 0$ in Z_n.
- As we will see, there are many other finite fields other than Z_p. Sometimes one writes $GF(k)$ for the finite field with k elements or other sources write F_k for the finite field with k elements. Your book uses GF except when talking about Z_p for primes p.

Finite fields, cont'd

- We define the characteristic of a field F to be the least number n such that

$$\underbrace{1+1+1+\ldots+1}_{n \text{ times}} = 0$$

if such an n exists and we say that the characteristic is 0 otherwise.

- R, C and the rationals have characteristic 0; Z_p has characteristic p for any prime p.

Lemma

Any finite field has characteristic p for some prime p and size p^n for some positive integer n.