Reducing Factoring to Order Finding - p1

Tuesday, November 13, 2018 8:33 AM

Quantum Algorithm for factoring (due to Peter Shor) is one the most celebrated achievements of quantum algorithms.

No known poly-time algorithm to factor numbers (despite significant effort).

Factoring is a fundamental problem in mathematics + hardness of factoring is the basis of some cryptographic schemes such as RSA.

Factoring Definition:

Input: integer N.

Output: $p_1\ p_2 \dots p_m$ $\quad l_1\ l_2 \dots l_m$ $\quad p_j$'s are prime

and $N = \prod_{j=1}^{m} (p_j)^{l_j}$

For example: $1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$

Note that it is sufficient to find a non-trivial divisor n because the algorithm can be applied recursively to n and N/n.

$18 \mid 1260 \rightarrow$ So apply recursively to 18 and $\frac{1260}{18} = 70$

Reducing Factoring to Order Finding - p2

Tuesday, November 13, 2018 8:34 AM

Input: integer N.

Output: $p_1\, p_2 \ldots p_m$ $\quad l_1\, l_2 \ldots l_m$ $\quad p_j$'s are prime

and $N = \prod_{j=1}^{m} (p_j)^{l_j}$

The size of the input to the problem is $O(\log N) = O$ (# digits or bits to denote N).

A naive classical algorithm will take time $O(\sqrt{N}\ \text{poly}(\log(N)))$

For $a = 1$ to $\sqrt{N}$. ← # loops $= \sqrt{N}$

if a evenly divides N return (a). ← time to determine if $a \mid N$ is polynomial in the # of bits to denote N.

Return ("prime").

Sophisticated algorithm such as the Field Sieve method take time $2^{O((\log N)^{1/3})}$

Still not practical for the size of numbers used in RSA in practice (~ 200 digits).

Reducing Factoring to Order Finding - p3

Tuesday, November 13, 2018 8:34 AM

Greatest Common Divisor $\gcd(x,y)$.

gcd (x,y) is the largest integer that evenly divides both x and y.

Can be computed efficiently by Euclid's Algorithm.

A helpful way to view the gcd:

$$x = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}.$$

$$y = p_1^{j_1} p_2^{j_2} \cdots p_m^{j_m}.$$

$$\gcd(x,y) = p_1^{\min(e_1,j_1)} \; p_2^{\min(e_2,j_2)} \cdots \; p_m^{\min(e_m,j_m)}$$

For example:

$$1320 = 2^3 \cdot 3 \cdot 5 \cdot 11 \qquad 2^3 \cdot 3^1 \cdot 5 \cdot 7^0 \cdot 11$$

$$1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7 \qquad 2^2 \cdot 3^2 \cdot 5 \cdot 7^1 \cdot 11^0$$

$$2^2 \cdot 3 \cdot 5 \cdot \cancel{7^0} \cdot \cancel{11^0}$$

You would never compute the gcd this way because finding the prime factorization is expensive.

Reducing Factoring to Order Finding - p4

Tuesday, November 13, 2018 8:34 AM

We will show that if you can solve the Order Finding Problem efficiently, then you can Factor efficiently.

≡ Factoring "reduces to" Order Finding.

The reduction rests on number-theoretic arguments and was known independently of quantum computation.

Order Finding:

Input: integers x & N such that $\gcd(x,N)=1$.
Output: Smallest r such that $x^r \equiv 1 \bmod N$.

this always exists if $\gcd(x,N)=1$.

$x \quad x^2 \bmod N \quad x^3 \bmod N \quad \ldots\ldots$

Will eventually get a repeat:

$$x^a \bmod N = x^b \bmod N \qquad b>a.$$

$$x^b - x^a = kN.$$
$$x^a(x^{b-a}-1) = kN.$$

if $\gcd(x,N)=1$ then

$$x^{b-a}-1 = k'N.$$
$$x^{b-a} \equiv 1 \bmod N.$$

Reducing Factoring to Order Finding - p5

Tuesday, November 13, 2018 8:34 AM

We will first show that finding a non-trivial square root of 1 mod N is sufficient to factor.

Lemma: given N composite such that $x^2 \equiv 1 \bmod N$ and $x \not\equiv \pm 1 \bmod N$ then we can factor N.

Proof: $x^2 - 1 \equiv 0 \bmod N$.

$$\left\{ \begin{aligned} x^2 - 1 &= kN. \qquad k \in \mathbb{Z}. \\ (x+1)(x-1) &= kN. \end{aligned} \right.$$

Since $x \not\equiv \pm 1 \bmod N$, neither $(x+1)$ nor $(x-1)$ is a multiple of N.

($x+1$ and $x-1$ each have some of N's prime factors).

$\gcd(x+1, N)$ and $\gcd(x-1, N)$ give non-trivial factors of N.

$\boxed{X}$

Given non-trivial $x^2 \equiv 1 \bmod N$ $\Longrightarrow$ Can find $n \mid N$, $1 < n < N$

Reducing Factoring to Order Finding - p6

Tuesday, November 13, 2018 9:30 AM

The algorithm for factoring will work as follows:

Check if $N = a^y$ for integers $a>1, y>1 \Rightarrow$ Return $(a, N/a)$
Otherwise, Repeat until success:

Pick x at random from $\{2, 3, \ldots, N-1\}$
If $\gcd(x, N) \neq 1$ then $\gcd(x,N)$ is a non-trivial divisor of $N \Rightarrow$ DONE!
Otherwise, compute $r = \text{ord}(x)$ ← this will be quantum

$x^{r/2} \neq 1 \bmod N$.

If r is odd, start again.
If r is even and $x^{r/2} = -1 \bmod N$ start again.

Otherwise $x^{r/2}$ is a non-trivial square root of $1 \bmod N \Rightarrow$ use it to factor N.

Need to lower bound the probability of success.

$\mathbb{Z}_N^* = \{x \bmod N \mid \gcd(x, N) = 1\}$

For example $\mathbb{Z}_{14}^* = \{1, 3, 5, \cancel{7}, 9, 11, 13\}$

$\mathbb{Z}_N^*$ is a group under multiplication mod N.

- closed under multiplication.
- $1 \in \mathbb{Z}_N^*$
- $\forall x \ \exists y \quad x \cdot y \equiv 1 \bmod N$ (every element has a mult. inverse).

\# elements in $\mathbb{Z}_N^* = \varphi(N)$ → Euler function.
$\lim_{N \to \infty} N/\varphi(N)$ is $O(\log \log N)$.

Reducing Factoring to Order Finding - p7

Tuesday, November 13, 2018 9:43 AM

What is the probability that an element x randomly chosen from $\mathbb{Z}_N^*$ has even order r and, if so, $x^{r/2} \neq -1 \mod N$.

Special Case: $N = p^\alpha$ for prime p and $\alpha > 1$.

Only multiples of p have a common divisor with N. and:

$$\varphi(N) = p^\alpha - \frac{N}{p} = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$$

$\varphi(N)$ must be even, so $\varphi(N) = 2^d (\text{odd } \#)$ $d \geq 1$.

We will use the following fact from number theory without proof:

The group $\mathbb{Z}_N^*$ for $N = p^\alpha$ has a generator g.

A generator is an element whose powers mod N are all the elements of $\mathbb{Z}_N^*$

$$\mathbb{Z}_N^* = \{ g, g^2, \ldots, \underline{g^{\varphi(N)}} \} \text{ (everything mod } N)$$

This has to be 1 since multiplying by g again brings us back to the beginning.

the order of g is $\varphi(N)$?

Reducing Factoring to Order Finding - p8

Tuesday, November 13, 2018 2:09 PM

$y \in_R \{1,2,3,\ldots,6\}$

$2^y \bmod N.$

Example $N = 3^2$

$\mathbb{Z}_N^* = \{1,2,4,5,7,8\}$ $\varphi(9) = 6.$

$g = 2$ is a generator.

$g^1 = 2$ $g^4 = 16 \bmod 9 = 7$

$g^2 = 4$ $g^5 = 32 \bmod 9 = 5$

$g^3 = 8$ $g^6 = 64 \bmod 9 = 1$

all mod 9.

One way to pick a random element from $\mathbb{Z}_N^*$

pick random $k \in \{1,\ldots,\varphi(N)\}$

take $g^k \bmod N.$

Reducing Factoring to Order Finding - p9

Tuesday, November 13, 2018 10:23 AM

$g^{\varphi(N)} \equiv 1 \mod N$.

($\varphi(N)$ is the smallest exponent that achieves this).

If $g^y \equiv 1 \mod N$ then y is a multiple of $\varphi(N)$.

(this follows from the fact that the order of g is $\varphi(N)$).

Take a random $x \in \mathbb{Z}_N^*$: $x \equiv g^k \mod N$.

Suppose r is the order of x :

$$x^r \equiv 1 \mod N \qquad g^{kr} \equiv 1 \mod N.$$

$kr = c \cdot \varphi(N) \Rightarrow kr$ is a multiple of $\varphi(N)$.

r is the smallest number such that kr is a multiple of $\varphi(N)$.

$\varphi(N) = 2 \cdot 2 \cdot 3 \cdot 5$

$k = 42 = 2 \cdot 3 \cdot 7$

$k \cdot 2 \cdot 5 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 7$

r contains all the prime factors in $\varphi(N)$ that are not already present in k.

$\varphi(N) = 2^d (\text{odd } \#)$.

(1) if k is odd $2^d \mid r$ (r even)

(2) if k is even $2^d \nmid r$. (r could be even or odd)

a randomly chosen x falls in to either category with prob. $1/2$.

r is even for at least half of the x's.

$k \cdot r = c \cdot 2^d (\text{odd } \#)$

k: odd

Reducing Factoring to Order Finding - p10

Tuesday, November 13, 2018 10:23 AM

To Summarize so far.

If $N = p^\alpha$ then $\underline{\varphi(N) = 2^d(\text{odd } \#)}$ for $d \geq 1$.

If x is chosen at random from $\mathbb{Z}_N^*$

$x = g^k \bmod N$.

Order of $x \triangleq r$.

2^d evenly divides r with prob $1/2$.

2^d does not evenly divide r with prob $1/2$.

$$\left[\text{For any } c\text{, the probability that } r = 2^c(\text{odd } \#) \text{ is } \leq 1/2\right]$$

Reducing Factoring to Order Finding - p11

Tuesday, November 13, 2018 2:20 PM

Now suppose $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$

Chinese Remainder Theorem

Let $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$

For any $(x_1, \ldots, x_m)$ where $0 \le x_i \le p_i^{\alpha_i} - 1$
there is exactly one $x \in \{0, 1, \ldots, N-1\}$
such that

$$x_i \equiv x \bmod p_i^{\alpha_i}$$

Ex: $N = 2^3 \cdot 3^2 \cdot 5 = 360$

$\Rightarrow (6, 7, 2)$ $\quad 0 \le 6 < 2^3 \quad 0 \le 7 < 3^2 \quad 0 \le 2 < 5$

$$\left.\begin{array}{l} 6 \equiv x \bmod 2^3 \\ 7 \equiv x \bmod 3^2 \\ 2 \equiv x \bmod 5 \end{array}\right\} \text{unique solution mod 360 is } x = 142.$$

One way to select a number in the range $0, \ldots, N-1$

for $i = 1$ to m select x_i independently at random from $\{0, \ldots, p_i^{\alpha_i} - 1\}$

x is unique solution to $x_i \equiv x \bmod p_i^{\alpha_i}$

Reducing Factoring to Order Finding - p12

Tuesday, November 13, 2018 2:28 PM

Back to original algorithm:

pick x at random from $\{0, 1, .., N-1\}$

if $\gcd(x, N) > 1 \Rightarrow$ DONE

else $x \in \mathbb{Z}_N^*$

$r \triangleq \text{order}(x)$.

Lower Bound

Probability that:

AND
(1) r is even
(2) $x^{r/2} \neq -1 \bmod N$

Upper Bound

Probability that

OR
(1) r is odd
(2) r is even and $x^{r/2} = -1 \bmod N$

(Will upper bound each event by $1/2^m$

$N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$

Define $N_i = p_i^{\alpha_i}$

X randomly chosen from $\{0, \dots, N-1\}$ $\longrightarrow$ $(X_1, X_2, \dots, X_m)$

$x_i = X \bmod N_i$

x_i chosen at random from $\{0, \dots, N_i - 1\}$.

$\gcd(x, N) = 1$ $\longrightarrow$ $\gcd(x_i, N_i) = 1$

$x \in \mathbb{Z}_N^*$ $\qquad$ $x_i \in \mathbb{Z}_{N_i}^*$

Reducing Factoring to Order Finding - p13

Friday, November 16, 2018 10:44 AM

$N_i = p_i^{\alpha_i}$

m independent random choices.

X randomly chosen from $\{0, \dots, N-1\}$ $\rightarrow$ $(x_1, x_2, \dots, x_m)$

$x_i = X \bmod N_i$

x_i chosen at random from $\{0, \dots, N_i - 1\}$.

$\gcd(X, N) = 1$ $\rightarrow$ $\gcd(x_i, N_i) = 1$

$X \in \mathbb{Z}_N^*$ $\quad$ $x_i \in \mathbb{Z}_{N_i}^*$

r = smallest value s.t. $X^r \equiv 1 \bmod N$

r_i = smallest value s.t. $(x_i)^{r_i} = 1 \bmod N_i$

Know: for any c, $\text{Prob}\left[r_i = 2^c (\text{odd } \#)\right] \leq \frac{1}{2}$

(1) Suppose r is odd.

$$X^r \equiv 1 \bmod N \longrightarrow X^r \equiv 1 \bmod N_i$$

$$\rightarrow (X \bmod N_i)^r = 1 \bmod N_i \longrightarrow (x_i)^r \equiv 1 \bmod N_i$$

So r_i evenly divides r.

If r is odd then each r_i must be odd.

A particular r_i is odd w.p. $\leq 1/2$

All the r_i are odd w.p. $\leq 1/2^m$

Reducing Factoring to Order Finding - p14

Friday, November 16, 2018 12:13 PM

(2) Suppose r is even and $x^{r/2} = -1 \bmod N$.

$$x^{r/2} = -1 \bmod N_i \rightarrow (x \bmod N_i)^{r/2} = -1 \bmod N_i$$

$$\rightarrow (x_i)^{r/2} = -1 \bmod N_i$$

$\Rightarrow$ r_i does not divide $r/2$

r_i does divide r.

If $r = 2^d(\text{odd }\#)$ then $\underline{r_i = 2^d}(\text{odd }\#)$

this happens for a particular i w.p. $\leq 1/2$.

This happens for all i, w.p. $\leq (1/2)^m$

Reducing Factoring to Order Finding - p15

Prob r is odd OR r is even and $x^{r/2} = -1 \bmod N$

$$\le \frac{1}{2^m} + \frac{1}{2^m} \le \frac{2}{2^m}.$$

The probability that the chosen x is "good" is $\left(1 - \frac{2}{2^m}\right)$

This is a terrible bound if $m=1$: $N = p^\alpha$
However this condition can be checked efficiently on a classical computer.