Using Period Finding to Factor an Integer

Peter Young

(Dated: November 1, 2019)

In this handout, we explain how finding the period of a certain function will enable us to factor integers. We will also illustrate the technique with a simple example. This will probably seem a strange approach for factoring, and is not the preferred method on a classical computer, but it is the method used by Shor in his quantum algorithm.

We take two large primes p and q and form the product

$$N = p\,q\,. \tag{1}$$

The goal is to find the factors p and q given only the product N. This is a problem which is hard classically. For applications in cryptography p and q may have around 600 digits (around 2000 bits). We proceed by choosing a random integer a which has no factors in common with N. Whether or not a and N have a common factor can be determined efficiently using Euclid's algorithm, which was described in the handout on RSA encryption `https://young.physics.ucsc.edu/150/rsa.pdf`. In the very unlikely event that a and N do have a common factor we have found a factor of N and the problem is solved. Otherwise we compute the following function

$$f(x) \equiv a^x \ (\mathrm{mod}\ N\,) \tag{2}$$

for $x = 1, 2, \cdots$. We are assuming that a and N have no common factors, and in this case one can show that eventually we will get $f(x) = 1$ for some value, $x = r$ say, so

$$a^r \ (\mathrm{mod}\ N) \equiv 1\,. \tag{3}$$

The function then repeats since

$$f(x+r) \equiv a^{x+r} \ (\mathrm{mod}\ N\,) \equiv a^x \ (\mathrm{mod}\ N\,) \times \ a^r \ (\mathrm{mod}\ N\,) \equiv a^x \ (\mathrm{mod}\ N\,) = f(x)\,, \tag{4}$$

using Eq. (3). Hence r is the period of the function.

We we illustrate with a simple example,

$$N = p\,q = 91, \quad \text{with factors } p = 13, q = 7. \tag{5}$$

We also take $a = 4$, which has no factors in common with 91. We plot $f(x) \equiv 4^x \ (\mathrm{mod}\ 91\,)$ in Fig. 1. The periodic nature is clear, and the period is found to equal 6 by inspection. Let's

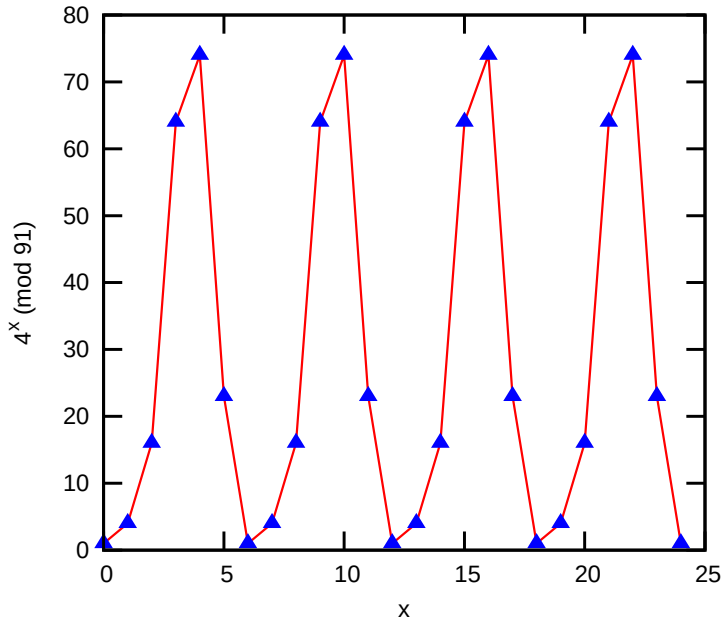

FIG. 1: The function $f(x) \equiv 4^x \pmod{91}$. The period is seen by inspection to equal 6.

make sure we understand how this figure is obtained by working out the values of $4^x \pmod{91}$ for $x = 1, 2, \cdots, 6$.

$$x = 1, \quad a^x = 4\,, \tag{6a}$$

$$x = 2, \quad a^x = 16\,, \tag{6b}$$

$$x = 3, \quad a^x = 64\,, \tag{6c}$$

$$x \equiv 4, \quad a^x \equiv 64 \times 4 = 256 \equiv 2 \times 91 + 74 \equiv 74 \ (\bmod 91)\,, \tag{6d}$$

$$x \equiv 5, \quad a^x \equiv 74 \times 4 = 296 \equiv 3 \times 91 + 23 \equiv 23 \ (\bmod 91)\,, \tag{6e}$$

$$x \equiv 6, \quad a^x \equiv 23 \times 4 \equiv 91 + 1 \equiv 1 \ (\bmod 91)\,. \tag{6f}$$

The plot in Fig. 1 seems to have a fairly regular behavior, but such smooth behavior is exceptional and occurs here because of the particular choice of parameters. Figure 2 shows a plot for the same value of N but with $a = 19$. This is a much more random looking figure, as is typical. In this case the period is $r = 12$. The apparently random shape of $f(x)$ means that one can not estimate the period by taking a few nearby values of x and extrapolating.

We now need to be lucky in two respects:

- The period r must be even. This means that $r/2$ is an integer and so is $a^{r/2}$. Hence we can

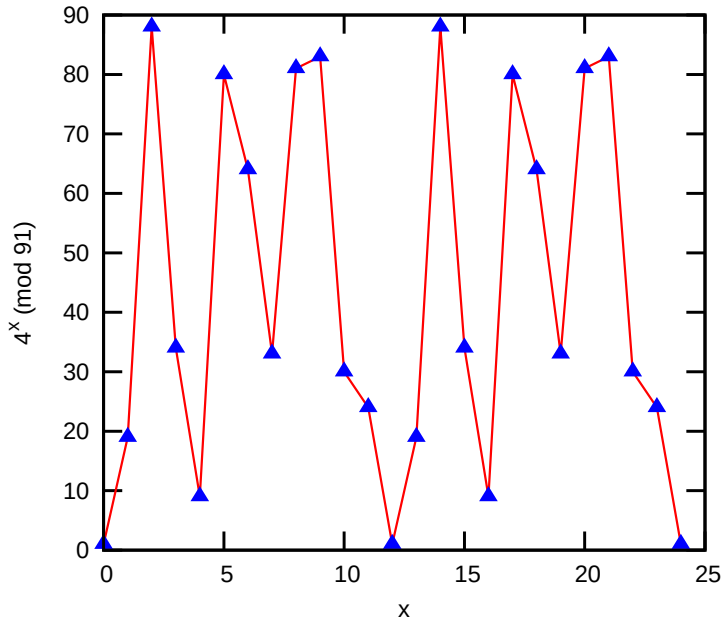

FIG. 2: The function $f(x) \equiv 19^x \pmod{91}$. The period is seen by inspection to equal 12.

write

$$0 \equiv a^r - 1 \equiv (a^{r/2} - 1)(a^{r/2} + 1) \pmod{p\,q}. \tag{7}$$

- We need that

$$a^{r/2} + 1 \not\equiv 0 \pmod{p\,q}. \tag{8}$$

It is automatically true that $a^{r/2} - 1 \not\equiv 0 \pmod{p\,q}$ because $x = r$ is the smallest power for which $a^x - 1 \equiv 0 \pmod{p\,q}$. Hence neither $a^{r/2} + 1$ nor $a^{r/2} - 1$ is divisible by $N = p\,q$ but, according to Eq. (7), their product is. Since p and q are primes, this is only possible if $a^{r/2} + 1$ is a multiple of one of the factors, p say, i.e. $a^{r/2} + 1 = Cp$, and $a^{r/2} - 1$ is a multiple of the other one q, i.e. $a^{r/2} - 1 = C'q$ (C and C' are constants).[1] Consequently p is the greatest common divisor of $N\,(= p\,q)$ and $a^{r/2} + 1\,(= Cp)$, and q is the greatest common divisor of N and $a^{r/2} - 1$. We can therefore find p and q using the Euclidean algorithm mentioned earlier.

[1] So $(a^{r/2} + 1)(a^{r/2} - 1) = CC'pq = CC'N$ which shows that $(a^{r/2} + 1)(a^{r/2} - 1)$ is a multiple of N. However, neither $a^{r/2} + 1$ nor $a^{r/2} - 1$ separately are a multiple of N since this is excluded, at least if $a^{r/2} + 1 \not\equiv 0 \pmod{p\,q}$ as assumed.

What are the odds that we will be doubly lucky in this way. According to Appendix M in Mermin, *Quantum Computer Science* the probability is greater than 0.5 for large N. If one is unlucky one tries a different choice for a. Since the probability of success is quite high at each attempt, one does not have to repeat the process very many times to succeed with very high probability.

Back to our example. For $N = 91, a = 4$ we found $r = 6$. Indeed we are lucky! This is even. Also $a^{r/2} + 1 = 65 \not\equiv 0 \pmod{91}$. So we are doubly lucky! However, this is not remarkable. As noted above the probability of this double luck is greater than 0.5 (at least for large N).

Hence one of the factors is the greatest common divisor of 91 and $a^{r/2} + 1 = 65$. The other factor is the greatest common divisor of 91 and $a^{r/2} - 1 = 63$.

Applying Euclid's algorithm[2]to $f_0 = 91, g_0 = 65$:

$$\begin{aligned} f_1 &= 65, \\ g_1 &= 91 - [91/65]\,65 = 91 - 65 = 26, \\ f_2 &= 26, \\ g_2 &= 65 - [65/26]\,26 = 65 - 52 = 13, \\ f_3 &= 13, \\ g_3 &= 26 - [26/13]\,13 = 26 - 26 = 0. \end{aligned} \tag{9}$$

Hence the GCD is $g_2 = 13$, which is indeed one of the factors of 91. By the same process the GCD of 63 and 91 is found to be 7, the other factor of 91.

[2] To determine the greatest common divisor (GCD) of f_0 and g_0 with $f_0 > g_0$ using Euclid's algorithm we iterate $f_{n+1} = g_n, g_n = f_n - [f_n/g_n]g_n$ starting with (f_0, g_0), where $[\cdots]$ means the integer part. One eventually gets $g_n = 0$ for some n, and the GCD is then g_{n-1}.