Topics: Discrete logarithms and applications.

4.1. It is easy to make silly mistakes when generating large primes p, q in view of constructing an RSA modulus $N = pq$, and some of these mistakes persist even when the numbers are "large enough" for cryptographic purposes.

Consider the number

$$N = 2\,100\,000\,000\,000\,000\,003\,260\,000\,000\,000\,000\,000\,533.$$

(a) Looking at the digit structure of N, find a quadratic polynomial $f(x) = ax^2 + bx + c$ with integer coefficients such that $f(10^k) = N$ for some suitable number of digits k.

[**Hint**: You can warm up on the smaller example $2\,100\,860\,033 = g(10^4)$, where g is a suitably-chosen quadratic polynomial with integer coefficients.]

(b) Factor $f(x)$ into a product of two linear factors with integer coefficients.

(c) Thus find p and q such that $N = pq$.

Solution.

(a) For the toy example in the hint we have $g(x) = 21x^2 + 86x + 33$.

For the given number N we have

$$N = 21 \cdot 10^{38} + 326 \cdot 10^{19} + 533 = f(10^{19}), \qquad \text{where } f(x) = 21x^2 + 326x + 533.$$

(b) This takes a bit of trial and error. It's likely that we want to split $21 = 3 \cdot 7$, so we're looking for

$$21x^2 + 326x + 533 = (3x + m)(7x + n) = 21x^2 + (3n + 7m) + mn.$$

Starting at the other end now, we have $533 = 13 \cdot 41$, and then the middle term gives us $m = 41$, $n = 13$.

In other words

$$f(x) = (3x + 41)(7x + 13).$$

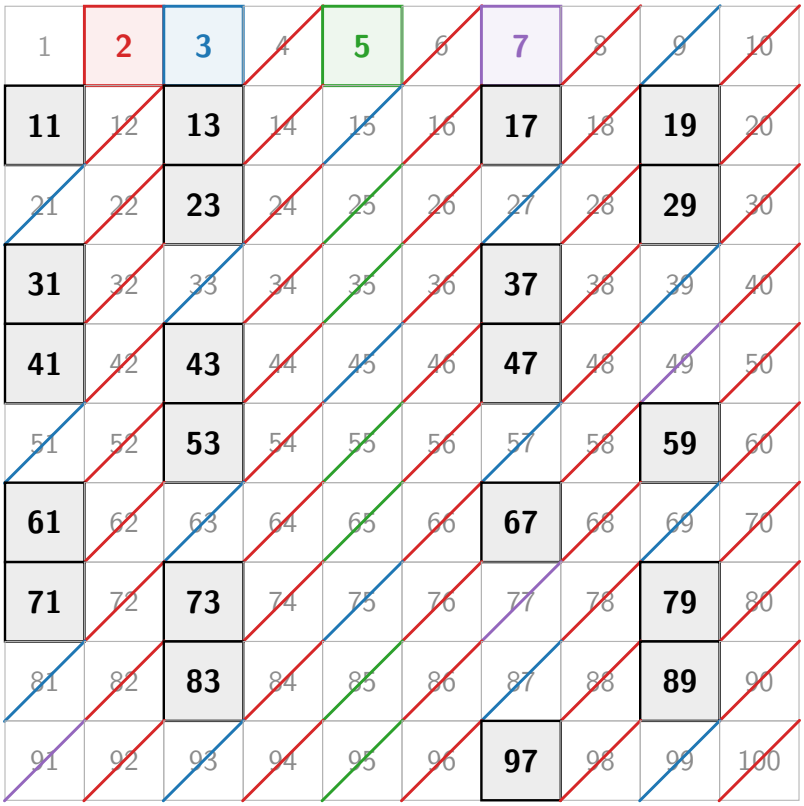
(c) We have

$$p = 3 \cdot 10^{19} + 41 = 30\,000\,000\,000\,000\,000\,041,$$
$$q = 7 \cdot 10^{19} + 13 = 70\,000\,000\,000\,000\,000\,013.$$

□

4.2. Recall that, given a positive real number B, a positive integer n is said to be *B-smooth* if all the prime divisors of n are $\leqslant B$.

Below is (the outcome) of the sieve of Eratosthenes for primes $\leqslant 100$. Build on this to run a sieving process that gives you all 6-smooth integers $\leqslant 100$.



Solution. Here is what you want to do: find the first prime that is not 6-smooth, namely 7. Cross this out (maybe along the other diagonal than the Eratosthenes crossings so you can distinguish it), then cross out all multiples of 7 up to 100. Just as with the original Eratosthenes, you should not need to do any multiplications, just keep adding 7.

Now go to the next prime, 11, and do the same.

You will have to do this for all the primes up to 47.

Once you are done, the boxes that you have not yourself crossed out are all the 6-smooth numbers. There are 34 of them:

$$1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 25, 27, 30, 32,$$
$$36, 40, 45, 48, 50, 54, 60, 64, 72, 75, 80, 81, 90, 96, 100. \quad \square$$

4.3. A function $f : \mathbf{Z}_{\geqslant 1} \longrightarrow \mathbf{Z}_{\geqslant 1}$ is *multiplicative* if for all $m, n \in \mathbf{Z}_{\geqslant 1}$, if $\gcd(m, n) = 1$ then $f(mn) = f(m)f(n)$.

(For example, we have seen that the Euler phi function ϕ is multiplicative.)

Prove that if f is multiplicative, then the function $\tilde{f} : \mathbf{Z}_{\geqslant 1} \longrightarrow \mathbf{Z}_{\geqslant 1}$ given by

$$\tilde{f}(n) = \sum_{d|n} f(d)$$

is multiplicative.

Solution. Suppose $\gcd(m, n) = 1$ and let $d \mid mn$. Set $b = \gcd(d, m)$ and $c = \gcd(d, n)$, then $d = bc$, $b \mid m$, $c \mid n$, and $\gcd(b, c) = 1$.

Therefore

$$\begin{aligned}\tilde{f}(mn) &= \sum_{d|mn} f(d) = \sum_{b|m} \sum_{c|n} f(bc) = \sum_{b|m} \sum_{c|n} f(b)f(c) \\ &= \left(\sum_{b|m} f(b)\right)\left(\sum_{c|n} f(c)\right) = \tilde{f}(m)\tilde{f}(n). \quad \square\end{aligned}$$

4.4.

(a) Prove that for any prime power p^e we have

$$\sum_{d|p^e} \phi(d) = p^e.$$

(b) Prove that for any $n \in \mathbf{Z}_{\geqslant 1}$ we have

$$\sum_{d|n} \phi(d) = n.$$

[**Hint**: Use part (a) and Tutorial Question 4.3.]

Solution.

(a) Straightforward, since the divisors of p^e are $d = 1, p, \ldots, p^e$:

$$\sum_{d|p^e} \phi(d) = \phi(1)+\phi(p)+\phi(p^2)+\cdots+\phi(p^e) = 1+(p-1)+p(p-1)+\cdots+p^{e-1}(p-1) = p^e.$$

(b) In the notation of Tutorial Question 4.3, we want to show that $\tilde{\phi}(n) = n$ for all $n \in \mathbf{Z}_{\geqslant 1}$.

Since ϕ is multiplicative, by Tutorial Question 4.3 so is $\tilde{\phi}$, so by factoring $n = p_1^{e_1} \ldots p_r^{e_r}$, it suffices to prove that $\tilde{\phi}(p^e) = p^e$ for any prime power p^e, which is precisely part (a). □

4.5. Fix an abelian group G and an element $g \in G$.

(a) Suppose Eve has a black box that solves the Diffie–Hellman problem: given (g^a, g^b), find g^{ab}.

Prove that Eve can use this to solve the ElGamal problem: given (g^a, g^b, mg^{ab}), it returns m.

(b) Prove the converse of (a), namely that if Eve has a box that solves the ElGamal problem, she can use it to solve the Diffie–Hellman problem.

(c) What if Eve's black box from part (b) is slightly defective and does not accept inputs where the third component is the identity element $1 \in G$?

Solution.

(a) This is obvious: Eve puts (g^a, g^b) in the box, gets g^{ab}, then computes $mg^{ab}(g^{ab})^{-1} = m$.

(b) Eve inputs $(g^a, g^b, 1)$ into the black box, which then returns $(g^{ab})^{-1}$. Eve can then compute the inverse of this element and get g^{ab}.

(c) Eve can pick a random non-identity element $x \in G$ and give the box (g^a, g^b, x). The box returns the corresponding m, which has the property that $mg^{ab} = x$. Then $g^{ab} = m^{-1}x$, which Eve can compute since she knows both m and x. □

4.6. Use the Pohlig–Hellman method to solve the discrete logarithm problem $h = g^e$ in $G = (\mathbf{Z}/19\mathbf{Z})^\times$, where $g = 2$ is a primitive root modulo 19 and $h = 5$.

[**Hint**: (a) Solve the DLP $h \equiv g^e \pmod{19}$ with $h = 5^9$ and $g = 2^9$. (b) Solve the DLP $h \equiv g^e \pmod{19}$ with $h = 5^2$ and $g = 2^2$.]

Solution. We have $N = \phi(19) = 19 - 1 = 18 = 2 \cdot 3^2$.

We therefore need to find $e \pmod 2$ and $e \pmod{3^2}$, then deduce e from the Chinese Remainder Theorem.

- First take $\ell_1 = 2$, $s_1 = 1$, $N_1 = N/2 = 9$. We solve for e in $h^9 \equiv (g^9)^e \pmod{19}$, in other words $5^9 \equiv (2^9)^e \pmod{19}$.

  Since 2 is a primitive root we know that it has order 18. In particular, $2^9 \not\equiv 1 \pmod{19}$, so we must have $2^9 \equiv -1 \pmod{19}$.

  On the other hand,

  $$5^9 = 5^8 \cdot 5 = (5^2)^4 \cdot 5 \equiv 6^4 \cdot 5 = (6^2)^2 \cdot 5 \equiv (-2)^2 \cdot 5 \equiv 20 \equiv 1 \pmod{19}.$$

  So to get $1 \equiv (-1)^e \pmod{19}$ we need $e \equiv 0 \pmod 2$.

- Now we take $\ell_2 = 3$, $s_2 = 2$, $N_2 = N/9 = 2$. We solve for e in $h^2 \equiv (g^2)^e \pmod{19}$, in other words $6 \equiv 4^e \pmod{19}$.

  We write $e = e_0 + 3e_1$. To get e_0, we solve $6^3 \equiv (4^3)^{e_0} \pmod{19}$. Since $6^3 \equiv (-2)\cdot 6 \equiv 7 \pmod{19}$ and $4^3 \equiv (-3) \cdot 4 \equiv 7 \pmod{19}$, the solution is $e_0 = 1$.

  To get e_1, we find $h_1 = 6 \cdot 4^{-1} \equiv 6 \cdot 5 \equiv 11 \pmod{19}$ and $g_1 = 7$, so we solve $11 \equiv 7^{e_1} \pmod{19}$, which gives $e_1 = 2$.

  Therefore $e = 1 + 3 \cdot 2 = 7$.

We have found that

$$\begin{aligned} e &\equiv 0 \pmod 2, \\ e &\equiv 7 \pmod 9, \end{aligned}$$

so using the Chinese Remainder Theorem we get $e = 16$.

It's easy to check this:

$$2^{16} \equiv (2^8)^2 \equiv ((2^4)^2)^2 \equiv ((-3)^2)^2 \equiv 9^2 \equiv 81 \equiv 5 \pmod{19}. \qquad \square$$

4.7. In this question, feel free to use either calculus-type reasoning or analysis-type reasoning, as you prefer.

Consider the real-valued function

$$L(x) = e^{\sqrt{(\log(x))(\log(\log(x)))}}.$$

(a) What is the implied domain of L? What is the range of L?

(b) Prove that for any $\varepsilon > 0$ we have

$$L(x) = O(x^\varepsilon),$$

in other words there exists a constant C (depending on ε but independent of x) such that

$$L(x) \leqslant Cx^\varepsilon \qquad \text{for all } x.$$

(c) Prove that for any $\alpha > 0$ we have

$$L(x) = \Omega((\log(x))^\alpha),$$

in other words there exists a constant D (depending on α but independent of x) such that

$$L(x) \geqslant D(\log(x))^\alpha \qquad \text{for all } x.$$

Solution.

(a) The implied domain is $[e, \infty)$.

The range is $[1, \infty)$. (It is clear that the range is contained in $[1, \infty)$, to prove equality we need to prove surjectivity. One option is to note that L is continuous and not bounded above, then use the Intermediate Value Theorem.)

(b) Since

$$\frac{\sqrt{\log(x)\log(\log(x))}}{\log(x)} \longrightarrow 0,$$

as $x \longrightarrow \infty$, given $\varepsilon > 0$ there exists $x_0 \in \mathbf{R}$ such that for $x > x_0$:

$$\frac{\sqrt{\log(x)\log(\log(x))}}{\log(x)} < \varepsilon \iff \sqrt{\log(x)\log(\log(x))} < \varepsilon \log(x).$$

Hence $L(x) < x^\varepsilon$ when $x > x_0$. Considering the interval $[e, x_0]$, the function $\frac{L(x)}{x^\varepsilon}$ is continuous and so attains a maximum M_ε. Set $C = \mathsf{max}\{1, M_\varepsilon\}$. Hence $L(x) \leqslant Cx^\varepsilon$ for all x.

(c) Since

$$\frac{\sqrt{\log(x)\log(\log(x))}}{\log(\log(x))} \longrightarrow \infty,$$

as $x \longrightarrow \infty$, given $\alpha > 0$ there exists $x_0 \in \mathbf{R}$ such that for $x > x_0$:

$$\frac{\sqrt{\log(x)\log(\log(x))}}{\log(\log(x))} > \alpha \iff \sqrt{\log(\log(x))} > \alpha \log(\log(x)).$$

Hence $L(x) > \log(x)^\alpha$ when $x > x_0$. Consdering the interval $[e, x_0]$, the function $\frac{L(x)}{\log(x)^\alpha}$ is continuous and so attains a minimum M_α. Set $D = \mathsf{min}\{1, M_\alpha\}$. Hence $L(x) \geqslant D(\log(x))^\alpha$ for all x. □