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.

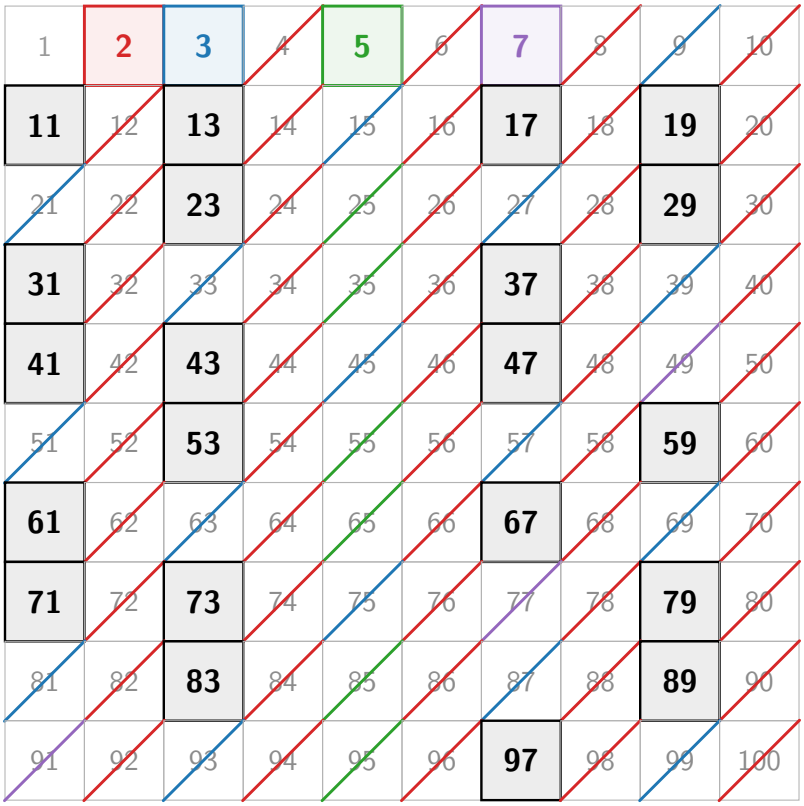
[**Hint**: You can warm up on the smaller example $2\,100\,860\,033 = g(10^4)$, where g is a suitably-chosen quadratic polynomial with integer coefficients.]

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

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

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 $\leqslant 100$.



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.

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.]

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 $1 \in G$?

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 $g = 2^2$.]

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

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