Instructions: Problems 2 and 9 are to be handed in by next Friday (theoretical ones on Moodle, programming ones on CoCalc).

1. Prove the Lemma from class stating that the order of any element in a finite group G divides the order of G.

2. Suppose that $n = p \cdot q$ is the product of two primes (but you are not given the factorization!). Show that knowledge of p, q is equivalent to knowledge of $\varphi(n)$.

3. Prove that if $\gcd(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \mod m$. *(Hint: You can first prove it for prime powers $m = p^n$ by induction on n, then deduce the general case.)*

4. (a) Prove that the Jacobi symbol satisfies $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$ for odd n.

   (Hint: Set $f(n) = (-1)^{(n^2-1)/8}$. Use multiplicativity of $f(n)$ to reduce to the case of prime $n = p$. Now let ζ denote a primitive 8-th root of unity and set $y = \zeta + \zeta^{-1}$. Show $y^2 = 2$ and evaluate y^p/y in the characteristic p field $\mathbb{F}_p(\zeta)$, distinguishing $p \equiv \pm 1 \mod 8$ and $p \equiv \pm 3 \mod 8$.)

   (b) Is 43691 a square mod 65537? Evaluate the Jacobi symbols $\left(\frac{936}{1443}\right)$ and $\left(\frac{936}{37055}\right)$.

   (Hint: use quad. reciprocity to evaluate the symbols).

   (c) Show that the number of solutions in $\mathbb{F}_p$ to the equation $ax^2 + bx + c = 0$ for $a \in \mathbb{F}_p^*$ is given by $1 + \left(\frac{b^2 - 4ac}{p}\right)$.

5. Find the smallest nonnegative solution to the system of congruences:

$$\begin{aligned} x &\equiv 12 \mod 31 \\ x &\equiv 87 \mod 127 \\ x &\equiv 91 \mod 255. \end{aligned}$$

6. Prove Wilson's theorem, stating that for p prime one has $(p-1)! \equiv -1 \mod p$. If $(n-1)! \equiv -1 \mod n$ does n have to be prime? If so, would this make a good way to test primality?

7. Find a sequence of positive integers n_j approaching infinity with $\lim_{j\to\infty} \varphi(n_j)/n_j = 1$ and a sequence of n_j for which $\lim_{j\to\infty} \varphi(n_j)/n_j = 0$.

8. Given positive integers N, g, A, prove the following algorithm computes $g^A \mod N$: (it provides a lower-storage variant of fast powering)

   (a) Set $a = g$ and $b = 1$.

   (b) Loop while $A > 0$:
   If $A \equiv 1 \mod 2$ set $b = b * a \mod N$.
   Set $a = a^2 \mod N$ and $A = \lfloor A/2 \rfloor$.

   (c) Return b, which equals $g^A \mod N$.

9. Use a program like SAGE to plot the powers $627^i \mod 941$ as a function of i. Do you see any patterns emerge? What about if you replace 941 by other (larger) prime numbers? *(Hint: use e.g., the Fermat prime $p = 65537$ and plot $7^i \mod p$. Then plot $7^{1024 \cdot i}$).*

10. (a) Write a program `timegcd(l,N)` that takes as input two integers l and N and does the following: you sample at random N pairs of l-bit integers (a, b) and measure the time it takes to compute the SAGE function `xgcd` on each pair. Then output the average of these times. *(Hint: use SAGE's `cputime()` command)*

    (b) For different values of l, plot the points $(l, timegcd(l, 100))$ and compare with the theoretical time estimates you have seen so far.