Exercise sheet 6, 22 December 2022

This exercise sheet is for self study. There are no instructions on 22 Dec. You can find a quiz on Canvas for checking the numerical answers. Of course you should ask yourself whether you understand what you are doing and why you are doing it.
For this exercise sheet you should not use your computer for more functions than a pocket calculator offers you (though with more digits) – unless explicitly stated.
At the end there are some practice exercises to check up on your knowledge on finite fields and groups. Skip these if you are confident in how to solve them – or keep them as a self test if you still need to (re-)learn the material.
There are many factorization algorithms, most obviously trial division where you trial divide by all primes up to $\sqrt{n}$ to find a factor of n, and the fastest ones run in subexponential time. Here we only cover one method, namely the $p-1$ method. This method works very efficiently for finding some primes and all you need for understanding it is Fermat's little theorem, which says that for all $0 < a < p$ we have $a^{p-1} \equiv 1 \bmod p$.
Said differently, $a^{p-1} - 1$ is a multiple of p and thus p divides $\gcd(a^{p-1} - 1, n)$. Computing gcds is fast, as is exponentiation, but we do not know $p-1$. What the $p-1$ method does is to pick a large exponent k, hoping that it is a multiple of $p-1$, and some base a and then compute $\gcd(a^k - 1, n)$. If indeed $a^k \equiv 1 \bmod p$ and at the same time $a^k \not\equiv 1 \bmod q$ then the gcd gives exactly p.
Note that in computing a^k you should use the square-and-multiply method *and* reduce modulo n as soon as your numbers get larger than n. This is compatible with the gcd computation because the first step there is to reduce modulo m,so you might as well do it along the way to keep the computation small. Do not forget the -1.
Typical choices for k are numbers with many small factors, such as $k = b!$ or $k = \text{lcm}\{1, 2, 3, \ldots, b\}$ for some bound b, which both guarantee that all primes up to b divide k. The two choices differ in how many times each of these primes divides k. The next exercises make you try the $p-1$ method for good choices of a and k. Keep in mind that it need not work, and will not work if both p and q are of the form $p = 2p' + 1$ and $q = 2q' + 1$ for p' and q' primes themselves. If you prefer to see a video explanation, please watch the end of `https://www.youtube-nocookie.com/embed/4PC3b52U1QU` with slides.
We also have some writeup at `https://facthacks.cr.yp.to/` for a talk we did at the Chaos Communication Congress on how to break RSA which has a bit on the $p-1$ method including code snippets.

1. For this exercise you should use a pocket calculator (or your computer with just basic functions). Use the $p-1$ method with $k = \text{lcm}\{1, 2, 3, \ldots, 6\}$ and base 2 to factor $n = 101617$.

2. For this exercise you can use your computer. Use the $p-1$ method with $k = \text{lcm}(1, 2, 3, 4, 5, \ldots, 50)$ and base 2 to factor $n = 400428248257$. If you get stuck on the precision of your computer, remember that the exponentiation is modulo n and that you learned the square-and-multiply method to deal with large exponents.

Alternatively, for the last step you can compute the exponentiation in pieces, using the factors of k.

3. The integer $p = 103$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange in a cyclic subgroup of $(\mathbb{Z}/p, +)$ with generator $g = 2$. You observe $h_a = 23$ and $h_b = 42$. What is the shared key of Alice and Bob?

4. The integer $p = 103$ is prime. You are the eavesdropper and know that Charlie and Dave use the Diffie-Hellman key-exchange in a cyclic subgroup of $(\mathbb{Z}/p, +)$ with generator $g = 2$. You observe $h_a = 21$ and $h_b = 39$. What is the shared key of Charlie and Dave?

5. The integer $p = 10007$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange in a cyclic subgroup of $(\mathbb{Z}/p, +)$ with generator $g = 1234$. You observe $h_a = 2345$ and $h_b = 4567$. What is the shared key of Alice and Bob?

6. This problem is about the DH key exchange. The public parameters are that the group is $(\mathbb{F}_{1009}^*, \cdot)$ and that it is generated by $g = 11$.
   (a) Compute the Diffie-Hellman public key belonging to the secret key $b = 548$.
   (b) Alice's Diffie-Hellman public key is $h_a = 830$. Compute the shared DH key with Alice using b from the previous part.
   (c) Alice and Bob keep the prime but change the generator to $g = 1008$. (This changes the subgroup generated). Simulate one round of DH key exchange. Why would you avoid this generator in practice?

7. The integer $p = 17$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange in $\mathbb{F}_{17}^*$ with generator $g = 3$. You observe $h_a = 12$ and $h_b = 14$. Use the Baby-Step Giant-Step algorithm to compute the secret key of Alice and Bob. Compute the shared key using both h_a^b and h_b^a.

8. Write all elements of $\mathbb{Z}/13$. For each element determine the order in $(\mathbb{Z}/13, +)$. What orders do you observe; what orders could be possible?

9. Write all elements of $\mathbb{Z}/6$. For each element determine the order in $(\mathbb{Z}/6, +)$. What orders do you observe; what orders could be possible?

10. Write all elements of $(\mathbb{Z}/13)^*$. For each element determine the order in $((\mathbb{Z}/13)^*, \cdot)$. What orders do you observe; what orders could be possible?

11. Write all elements of $(\mathbb{Z}/6)^*$. For each element determine the order in $((\mathbb{Z}/6)^*, \cdot)$. What orders do you observe; what orders could be possible?

12. Show that $\mathbb{F}_{61}^* = \langle 2 \rangle$, i.e. show that the order of 2 in $\mathbb{F}_{61}$ is 60.

13. Determine the smallest generator $g \in (\mathbb{Z}/4969)^*$ that is larger than 1000. Do this by testing whether $1000 + i$ is a generator, starting from $i = 1$ and incrementing i if it is not. Try to make each test as cheap as possible. For this exercise I suggest you use modular exponentiation on your computer but don't just ask it for the order.