Adv Topics 2 (Lesieutre)
August 24, 2021

Problem 1. This week, we'll think about cryptography. Divide yourselves into two groups, and imagine that you want to be able to pass coded messages back and forth without your teacher being able to read them, even if they are intercepted.

If you could agree on a shared 4-digit secret key (unknown to the teacher), you could use this to encode the message.

a) Try to have the two groups agree on a secret key by sending some messages back and forth. Remember, I get to read the messages! What is your strategy?

b) Now imagine that you are trying to agree on a key with a stranger in Amazon's payments processing department, and that anyone on the internet could listen in. Can you think of a new method?

Problem 2. Compute the following modular quantities:

a) 19 mod 4

b) $(232 + 37)$ mod 11 (There are two ways you could do this – do you get the same answer? Why?)

Problem 3. Compute the following modular exponentials.

a) $19^2 \bmod 11$

b) $19^3 \bmod 11$

c) $19^4 \bmod 11$

d) $19^8 \bmod 11$

e) $19^{16} \bmod 11$

f) $19^{21} \bmod 11$

g) $19^{73} \bmod 11$

Problem 4. Describe a general method for compute $a^b \bmod n$ without doing b separate multiplications. (For the computer scientists: roughly how many times do you need to multiply?)

Problem 5. Use Diffie–Hellman key exchange to generate a shared two-digit key with a friend.

Problem 6. How secure is this, anyway? Think through the Diffie–Hellman algorithm. Which quantities are known to someone eavesdropping on your messages? What else would they need to know or calculate in order to obtain the shared key?

Problem 7. Let $\phi(n)$ denote the Euler ϕ function, the number of integers less than n and coprime to n.

a) Compute $\phi(10)$.

b) Compute $\phi(13)$.

c) What is $\phi(p)$, if p is a prime number?

d) What is $\phi(pq)$, if p and q are both prime numbers?

e) Compute $7^{12} \pmod{13}$ using our method from before. Does your answer agree with the calculation of Fermat's little theorem?

Problem 8. You plan to receive an encrypted message from me using RSA. First, you need to pick two large primes. If you want to send the message in a single piece (instead of splitting it into smaller pieces), their product needs to have as many digits as the message will have. (To be totally safe, you need each prime to have that many digits, just in case the message is not coprime to n. Let's not.)

Say you chose the two primes

$$\begin{aligned} p &= 1500450271, \\ q &= 3628273133. \end{aligned}$$

a) First, you need to compute the product $n = pq$ as well as $\phi(n)$. What is $\phi(n)$?

b) Next you need to generate the encryption and decryption keys. You can either pick d and calculate e, or vice versa. Let's say we pick $d = 65537$, and solve for e. What is e? (We'll want to ask a computer to do this.)

c) With those numbers in hand, you publish n and e, but keep d secret. I now write my message in the form of a number M and compute $E = M^e \pmod{n}$. Again this is easy, because I can use fast modular exponentiation. Here's the message I send you:

$$E = 5219361229139918678$$

d) Now decrypt the message given in the previous part. First find M from E using the RSA algorithm. Note that the decryption key is $d = 65537 = 2^{16} + 2^0$, so you can find this using the repeated squaring algorithm mod n without very much work, as long as you can square mod n.

e) To turn it into text, write M as a base-10 number. Each two digits in M correspond to an English letter via the code $A = 01$, $B = 02$, $C = 03$, $\ldots$, $Z = 26$. What is the message?