Grade 11/12 Math Circles

February 23, 2022

Cryptography, Part 2 - Solutions

Exercise Solutions

Exercise 1

Compute the following greatest common divisors by factoring the integers as products of primes.

(a) $\gcd(11, 31)$

(b) $\gcd(629, 357)$

(c) $\gcd(36652, 68552)$

Exercise 1 Solution

(a) Both 11 and 31 are prime numbers, so they have no prime factors in common. Note that 1 divides every number, and so 1 must be the largest number that divides both the primes 11 and 31. In other words, $\gcd(11, 31) = 1$.

(b) We try to factor both of 629 and 357 into primes by trial divison. After some time, we get

$$629 = 17 \cdot 37$$
$$357 = 3 \cdot 7 \cdot 17.$$

Only 17 is a prime common to both factorizations, and so $\gcd(629, 357) = 17$.

(c) Again, we aim to factor both 36652 and 68552 into primes. With some trial-and-error division, we get

$$36652 = 2 \cdot 2 \cdot 9163 = 2 \cdot 2 \cdot 7 \cdot 7 \cdot 187 = 2 \cdot 2 \cdot 7 \cdot 7 \cdot 11 \cdot 17$$
$$68552 = 2 \cdot 2 \cdot 2 \cdot 8569 = 2 \cdot 2 \cdot 2 \cdot 11 \cdot 779 = 2 \cdot 2 \cdot 2 \cdot 11 \cdot 19 \cdot 41.$$

We see that the overlap between the two factorizations is two 2s and an 11, so $\gcd(36652, 68552) = 2 \cdot 2 \cdot 11 = 44$.

Exercise 2

Use the Euclidean algorithm to calculate the following gcds:

(a) $\gcd(36652, 68552)$ (this was done in Exercise 1 in another way)

(b) $\gcd(4019881, 10394)$

Exercise 2 Solution

(a) We start by dividing 68552 by 36652 with remainder, which gives us

$$68552 = 1 \cdot 36652 + 31900.$$

Next, we take 36652 and divide it by the remainder 31900:

$$36552 = 1 \cdot 31900 + 4752.$$

Continuing, we take 31900 and divide it by the new remainder 4752:

$$31900 = 6 \cdot 4752 + 3388.$$

We now continue this process of taking the divisor from the previous step and dividing it by the remainder from the previous step, until we reach a remainder of 0.

$$\begin{aligned} 4752 &= 1 \cdot 3388 + 1364 \\ 3388 &= 2 \cdot 1364 + 660 \\ 1364 &= 2 \cdot 660 + 44 \\ 660 &= 15 \cdot 44 + 0 \end{aligned}$$

From here, the last non-zero remainder is our gcd (in this case, 44). We conclude that $\gcd(36652, 68552) = 44$, which should confirm one of your answers from Exercise 1!

(b) As above, we repeatedly perform divisions with remainder, starting with 4019881 by 10394,

and then dividing the divisor from each step by the remainder from that same step.

$$\begin{aligned} 4019881 &= 386 \cdot 10394 + 7797 \\ 10394 &= 1 \cdot 7797 + 2597 \\ 7797 &= 3 \cdot 2597 + 6 \\ 2597 &= 432 \cdot 6 + 5 \\ 6 &= 1 \cdot 5 + 1 \\ 5 &= 5 \cdot 1 + 0. \end{aligned}$$

The last non-zero remainder is 1, and so $\gcd(4019881, 10394) = 1$.

Exercise 3

Using the Extended Euclidean algorithm, find integers x and y satisfying each of the following equations:

(a) $28x + 12y = 4$ (**Hint:** We calculated $\gcd(28, 12)$ using the Euclidean algorithm earlier.)

(b) $63x + 91y = 7$

Exercise 3 Solution

(a) Earlier in the lesson, we checked that $\gcd(28, 12) = 4$ using the following divisions with remainder:

$$\begin{aligned} 28 &= 2 \cdot 12 + 4 \\ 12 &= 3 \cdot 4 + 0. \end{aligned}$$

When we ignore the last line and re-write the first one with the remainder by itself,

$$4 = 28 - 2 \cdot 12,$$

we have already written 4 as a multiple of 28 plus a multiple of 12. Thus, we see that a solution to $28x + 12y = 4$ is $x = 1$ and $y = -2$.

(b) Here, we must first calculate $\gcd(63, 91)$ using the Euclidean algorithm. We do this with

the following divisions with remainder:

$$91 = 1 \cdot 63 + 28$$
$$63 = 2 \cdot 28 + 7$$
$$28 = 4 \cdot 7 + 0.$$

The last non-zero remainder is 7, so this verifies $\gcd(63, 91) = 7$. Now, we ignore the last line and solve for the remainder in each of the first two equations, writing them in reverse order:

$$7 = 63 - 2 \cdot 28$$
$$28 = 91 - 1 \cdot 63.$$

If we substitute the second equation into the first in place of 28, we can then write 7 as a multiple of 63 plus a multiple of 91, as needed:

$$\begin{aligned} 7 &= 63 - 2 \cdot 28 \\ &= 63 - 2 \cdot (91 - 1 \cdot 63) \\ &= 63 - 2 \cdot 91 + 2 \cdot 63 \\ &= 3 \cdot 63 - 2 \cdot 91. \end{aligned}$$

We now see that an integer solution to $63x + 91y = 7$ is $x = 3, y = -2$.

Exercise 4

Try this for yourself! Choose primes p and q, and calculate the public and private keys. If you have a friend to try this with, have them send you a ciphertext and try to decrypt it.

Exercise 4 Solution

Answers will vary.

Problem Set Solutions

1. Which of the following numbers are prime? For the ones that aren't prime, factor them as a product of primes.
   (a) 101
   (b) 119
   (c) 127

Solution:
(a) The number 101 is prime. You can verify this using trial division – if 101 were not prime, it would have a prime factor smaller than 11. (Can you explain why?) But 101 is not divisible by any primes smaller than 11, so it must be prime.
(b) The number 119 is not prime, because it factors as $119 = 7 \cdot 17$.
(c) The number 127 is prime. Just as you can argue in part (a), if this number were not prime, it would have a prime factor smaller than 13. But 127 is not divisible by any primes smaller than 13.

2. (a) For any positive integer a, what is $\gcd(a, 0)$ equal to?
   (b) Calculate $\gcd(15, 27)$ using the Euclidean algorithm.
   (c) Calculate $\gcd(61783, 4019881)$ using the Euclidean algorithm.

Solution:
(a) For any positive integer a, $\gcd(a, 0) = a$. Indeed, a divides itself, and a divides 0 because $0 = a \cdot 0$. Any integer larger than a cannot divide a, so a is indeed the *greatest* common divisor of a and 0.
(b) We perform divisions with remainder, starting with dividing 27 by 15.

$$27 = 1 \cdot 15 + 12$$
$$15 = 1 \cdot 12 + 3$$
$$12 = 4 \cdot 3 + 0.$$

We see that 3 is the last non-zero remainder, so $\gcd(15, 27) = 3$.

(c) Again, we perform divisions with remainder, starting with dividing 4019881 by 61783.

$$4019881 = 65 \cdot 61783 + 3986$$
$$61783 = 15 \cdot 3986 + 1993$$
$$3986 = 2 \cdot 1993 + 0.$$

We see that 1993 is the last non-zero remainder, so $\gcd(61783, 4019881) = 1993$.

3. Find integers x and y solving the following equations.

(a) $15x + 27y = 3$. (**Hint:** We've done half the work in the previous question.)

(b) $17x + 31y = 1$.

(c) $17x + 31y = 4$. (**Hint:** This requires a little more than just the Extended Euclidean algorithm. How can you work with the answer obtained in part (b) to get an answer here?)

Solution:

(a) Starting from the Euclidean algorithm work from question 2(b), we have

$$27 = 1 \cdot 15 + 12$$
$$15 = 1 \cdot 12 + 3$$
$$12 = 4 \cdot 3 + 0.$$

Leaving out the last line, solving for the remainders, and writing them in reverse order, we get

$$3 = 15 - 1 \cdot 12$$
$$12 = 27 - 1 \cdot 15.$$

Substituting the second equation into the first, we get

$$\begin{aligned} 3 &= 15 - 1 \cdot 12 \\ 3 &= 15 - 1 \cdot (27 - 1 \cdot 15) \\ 3 &= 2 \cdot 15 - 1 \cdot 27. \end{aligned}$$

This gives us the solution $x = 2$ and $y = -1$ to the equation $15x + 27y = 3$.

(b) Here, we first have to run the Euclidean algorithm on 17 and 31, which gives us

$$\begin{aligned} 31 &= 1 \cdot 17 + 14 \\ 17 &= 1 \cdot 14 + 3 \\ 14 &= 4 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Removing the last line, solving for the remainders, and writing them in reverse order, we get

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ 2 &= 14 - 4 \cdot 3 \\ 3 &= 17 - 1 \cdot 14 \\ 14 &= 31 - 1 \cdot 17. \end{aligned}$$

Substituting each line one at a time, we get

$$\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
&= 3 - 1 \cdot (14 - 4 \cdot 3) \\
&= 3 - 1 \cdot 14 + 4 \cdot 3 \\
&= 5 \cdot 3 - 1 \cdot 14 \\
&= 5 \cdot (17 - 1 \cdot 14) - 1 \cdot 14 \\
&= 5 \cdot 17 - 5 \cdot 14 - 1 \cdot 14 \\
&= 5 \cdot 17 - 6 \cdot 14 \\
&= 5 \cdot 17 - 6 \cdot (31 - 1 \cdot 17) \\
&= 5 \cdot 17 - 6 \cdot 31 + 6 \cdot 17 \\
&= 11 \cdot 17 - 6 \cdot 31.
\end{aligned}$$

This gives us the solution $x = 11$ and $y = -6$ to the equation $17x + 31y = 1$.

(c) Given our work in part (b), there is just one more thing to do. We already know that $17 \cdot 11 + 31 \cdot (-6) = 1$, and if we multiply both sides by 4, we get

$$17 \cdot (11 \cdot 4) + 31 \cdot (-6 \cdot 4) = 4.$$

This gives a solution $x = 11 \cdot 4 = 44$ and $y = -6 \cdot 4 = -24$ to the equation $17x + 31y = 4$.

4. Compute the following values of the Euler phi function.
   (a) $\phi(7)$
   (b) $\phi(15)$
   (c) $\phi(27)$
   (d) $\phi(30)$
   (e) $\phi(p^k)$, where p is a prime number and k is a positive integer.

Solution:

(a) Since 7 is prime, we apply the formula for $\phi(p)$ where p is prime from Example 5.

This gives us $\phi(7) = 7 - 1 = 6$.

(b) Since $15 = 3 \cdot 5$ is the product of two different primes, we can use the formula for $\phi(n)$ in the case discussed in Example 6. This gives us $\phi(15) = (3-1)(5-1) = 2 \cdot 4 = 8$.

(c) Since $27 = 3^3$, we haven't discussed a formula for $\phi(n)$ that will work here. We could try all the numbers between 1 and 27 and take gcds, but let's be a little bit more clever.

Since 3 is the only prime dividing 27, we get $\gcd(m, 27) \neq 1$ exactly when m is a multiple of 3. So, we just have to count the number of multiples of 3 between 0 and 26 and subtract them from 27 to get the answer. Now, there are exactly nine multiples of 3 in that range:

$$3, 6, 9, 12, 15, 18, 21, 24, 27.$$

Hence $\phi(27) = 27 - 9 = 18$.

(d) Notice that $30 = 2 \cdot 3 \cdot 5$, so we haven't discussed any tricks for calculating $\phi(30)$ that will compute it instantly. But again, given an integer m between 1 and 30, we will have $\gcd(m, 30) \neq 1$ exactly when m is a multiple of either $2, 3$, or 5. So, let's start by removing all multiples of 2 from the list of integers from 1 to 30, giving

$$1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29.$$

From that list, we now remove the multiples of 3:

$$1, 5, 7, 11, 13, 17, 19, 23, 25, 29.$$

And finally, we take away the multiples of 5:

$$1, 7, 11, 13, 17, 19, 23, 29.$$

This remaining list gives all the integers m between 1 and 30 for which $\gcd(m, 30) = 1$. There are eight integers on this list, so $\phi(30) = 8$.

(e) Here, we can use the same approach that worked for calculating $\phi(27)$, which was also a power of a prime number. Knowing that p is the only prime factor of p^k, if

we have an integer m between 1 and p^k, we know that $\gcd(m, p^k) \neq 1$ exactly when m is a multiple of p.

There are p^k integers from 1 to p^k, and exactly $\frac{p^k}{p} = p^{k-1}$ of them are multiples of p, namely all integers of the form np, where n ranges from 1 up to p^{k-1}. Subtracting off all of these multiples of p from the total, we get $p^k - p^{k-1}$ integers m between 1 and p^k not divisible by p. This tells us

$$\phi(p^k) = p^k - p^{k-1}.$$

Notice that this agrees with the $k = 1$ case worked out in Example 5, as well as the case $p = 3, k = 3$ that we solved in part (c).

5. Modular arithmetic is good for much more than RSA. If an equation is true in the integers, we can "reduce it mod n" to get a congruence mod n that is also true. This is more useful in the other direction: if we start with an equation and prove it has no solutions mod n for some choice of n, then there are no integer solutions. This helps because we can exhaustively try every possibility for the variables mod n – there are only n different choices for each variable that would give a distinct result.

   Prove that each of the following equations has no integer solution by showing each one has no solutions mod n for a small choice of n (in each case, you can take $n \leq 5$.)

   (a) $6x + 21y = 2$

   (b) $5y = x^2 + 2$

   (c) $x^2 + y^2 = 31$

Solution:

(a) Here, we take the equation and reduce it modulo 3. This gives us

$$6x + 21y \equiv 2 \pmod 3.$$

Now, notice that both 6 and 21 are congruent to 0 mod 3. This means $6x \equiv 0 \pmod 3$ and $21y \equiv 0 \pmod 3$. The congruence above then simplifies to

$$0 + 0 \equiv 2 \pmod 3.$$

In turn, this says $0 \equiv 2 \pmod 3$. By definition, this means $3 \mid (0-2)$. This is impossible, as -2 is not divisible by 3. This shows that the congruence has no solution modulo 3, which means the original equation has no solution either.

(b) For this one, we take the equation and reduce it modulo 5. Since $5y \equiv 0 \pmod 5$ no matter what value we take for the integer y, we find that the congruence $5y \equiv x^2+2 \pmod 5$ reduces to

$$0 \equiv x^2 + 2 \pmod 5.$$

Now, there are only five "different" integers modulo 5, namely $0, 1, 2, 3, 4$. Let's try them all as possible values of x to see what x^2+2 comes out to:

$$\begin{aligned}
0^2 + 2 &\equiv 2 \pmod 5 \\
1^2 + 2 &\equiv 3 \pmod 5 \\
2^2 + 2 &\equiv 6 \equiv 1 \pmod 5 \\
3^2 + 2 &\equiv (-2)^2 + 2 \equiv 6 \equiv 1 \pmod 5 \\
4^2 + 2 &\equiv (-1)^2 + 2 \equiv 3 \pmod 5.
\end{aligned}$$

We just tried all possible values for x modulo 5, and none of them gave us $x^2+2 \equiv 0 \pmod 5$. Therefore, the congruence has no solutions, which implies the equation $5y = x^2 + 2$ has no integer solutions.

(c) For this equation, reducing modulo 4 works. When we do this, we end up with

$$x^2 + y^2 \equiv 31 \equiv 3 \pmod 4.$$

Since $0, 1, 2, 3$ represent all the different possible values modulo 4, we can try each of these as values for x to see what the possibilities for x^2 will be:

$$\begin{aligned}
0^2 &\equiv 0 \pmod 4 \\
1^2 &\equiv 1 \pmod 4 \\
2^2 &\equiv 4 \equiv 0 \pmod 4 \\
3^2 &\equiv 9 \equiv 1 \pmod 4.
\end{aligned}$$

Therefore, no matter what x is, we know that $x^2 \equiv 0 \pmod 4$ or $x^2 \equiv 1 \pmod 4$.

Similarly, these are the only two possible values for y^2 modulo 4. Putting that together, the possibilities for $x^2 + y^2$ modulo 4 will be:

$$\begin{aligned} 0 + 0 &\equiv 0 \pmod 4 \\ 0 + 1 &\equiv 1 \pmod 4 \\ 1 + 0 &\equiv 1 \pmod 4 \\ 1 + 1 &\equiv 2 \pmod 4 \end{aligned}$$

None of these possibilities gives us an answer of 3 modulo 4, so $x^2 + y^2 \equiv 3 \pmod 4$ has no solutions. In turn, this implies $x^2 + y^2 = 31$ has no integer solutions either.

6. In RSA, Nick is not supposed to reveal $\phi(N)$, because knowing it allows everybody to calculate Nick's private key. It's time to put on our cryptanalysis hats and try to break the system. If we know p and q, the two factors of N, it becomes easy to calculate $\phi(N)$. However, as we know, finding those factors is really hard. Maybe there's an easier way to calculate $\phi(N)$? We're going to see the answer is no.

   (a) Suppose you have a magic machine that takes N and instantly calculates $\phi(N)$. How can you use the values of N and $\phi(N)$ to calculate $p + q$?

   (b) Once you know both $p + q$ and $N = pq$, how can you calculate both p and q? (**Hint:** Consider the quadratic formula applied to the polynomial $x^2 - (p + q)x + pq$.)

   What this means is that an efficient way for calculating $\phi(N)$ leads to an efficient way of factoring N, and everyone believes that factorization is really hard.

Solution:

(a) If we have the values of $N = pq$ and $\phi(N) = (p-1)(q-1) = pq-p-q+1$, the value of $p+q$ is easy to obtain. Indeed, notice that $N-\phi(N) = pq-(pq-p-q+1) = (p+q)-1$.

So, if we know N and a machine has given us the value of $\phi(N)$, then we can put $N - \phi(N) + 1$ into a calculator and find the value of $p + q$.

(b) As suggested in the hint, let's see what the quadratic formula says about the roots

of the polynomial $x^2 - (p+q)x + pq$. By that formula, the roots are

$$\begin{aligned} x &= \frac{-(-(p+q)) \pm \sqrt{(-(p+q))^2 - 4pq}}{2} \\ &= \frac{(p+q) \pm \sqrt{p^2 + 2pq + q^2 - 4pq}}{2} \\ &= \frac{(p+q) \pm \sqrt{p^2 - 2pq + q^2}}{2} \\ &= \frac{(p+q) \pm \sqrt{(p-q)^2}}{2} \\ &= \frac{(p+q) \pm |p-q|}{2}. \end{aligned}$$

The absolute value makes things a little complicated, but because of the $\pm$ in the quadratic formula, in every case the two roots come out to be p and q. Therefore, if you use the known numbers $N = pq$ and $p + q$, applying the quadratic formula to $x^2 - (p+q)x + pq$ gives the values of p and q as the answers. This may be the single coolest application of the quadratic formula ever to exist!

7. Like any cryptosystem, the security of RSA can be compromised if used incorrectly. Suppose Nick and Bahaa have the same value of N, but different encryption exponents e_1 and e_2.

   (a) Explain how Nick and Bahaa can work out each other's private keys, and therefore read each other's encrypted messages.

   (b) Suppose Shefaza comes along and sends the same message M to both Nick and Bahaa (maybe it's Shefaza's credit card number). Suppose also that $\gcd(e_1, e_2) = 1$. Now, let's say Diana comes along and reads the ciphertexts that Shefaza sent to Nick and Bahaa, say $C_1 \equiv M^{e_1} \pmod{N}$ and $C_2 \equiv M^{e_2} \pmod{N}$.

   Explain how Diana can use this information to recover Shefaza's plaintext M.

   Hint: Running the Extended Euclidean algorithm on e_1 and e_2 allows Diana to find integers x and y such that $e_1 x + e_2 y = 1$. How can this information help her recover M?

Solution:

(a) Because Nick and Bahaa have both chosen the same value of N, both of them started by choosing the same primes p and q to create N. In particular, both Nick and Bahaa know the value of $\phi(N)$. Because of this, if Nick used exponent e_1 and Bahaa used

exponent e_2, Nick could look up e_2 and find Bahaa's decryption exponent d_2 by running the Extended Euclidean algorithm on $\phi(N)$ and e_2. In the same way, Bahaa can calculate Nick's decryption exponent d_1.

(b) As mentioned in the hint for the question, since $\gcd(e_1, e_2) = 1$, Diana can use the known values of e_1 and e_2 to find integers x and y such that $e_1x + e_2y = 1$, by running the Extended Euclidean algorithm.

At this point, Diana should take the ciphertexts C_1 and C_2 that she intercepted and compute $C_1^x \cdot C_2^y \pmod{N}$. Here is what happens when she does this:

$$C_1^x \cdot C_2^y \equiv (M^{e_1})^x \cdot (M^{e_2})^y \equiv M^{e_1x} \cdot M^{e_2y} \equiv M^{e_1x+e_2y} \equiv M^1 \pmod{N}.$$

So, if Diana calculates the unique integer M between 0 and $N-1$ such that $M \equiv C_1^x \cdot C_2^y \pmod{N}$, then M will be the desired plaintext.

Remark: There's a minor point to mention here: we only talked about what it means to raise numbers to positive exponents mod N. Here, x or y could be negative. There's a way to make sense of negative exponents mod N, which you can investigate if you are curious! But don't worry: the argument given here can indeed be made valid.