MATH 4440/5440 Assessment, Module 3 (RSA, Primality, Factoring, Euclidean Algorithm)

Katherine Stange, CU Boulder, Fall 2020

Honor Code Rules

Assessments are open book, but are to be completed on your own without collaboration. To be specific, you may use your course notes, textbook, course website resources, course videos. You may not use the internet beyond the course websites. You may not ask anyone else for help (except your professor), including other humans, or posting/entering your question or any part of it into the internet. You may not share the questions or answers with anyone else. You may not use calculators (even from the course websites) unless explicitly permitted in the question.

Have you read, understood, and followed the honor code rules above?

YES / *NO*

Some instructions on formatting.

You may use the accompanying LaTeX source document to produce LaTeX'ed answers. You may typeset answers separately. You may print the pages and solve the questions on them by hand. You may handwrite answers on separate sheets. You may upload PDF or image files (JPG or PNG). No matter what you do, just make sure it is clearly and easily legible before you upload it to canvas.

1 Question 1

(10 points) Find the gcd of 715 and 3620.

You may not use a calculator/computer. Please show your work neatly and **show all steps**. When you are done, double-check your work.

Solution. The gcd is determined by the Euclidean algorithm:

$$\begin{aligned} 3620 &= 5 \cdot 715 + 45 \\ 715 &= 15 \cdot 45 + 40 \\ 45 &= 1 \cdot 40 + 5 \\ 40 &= 8 \cdot 5 + 0 \end{aligned}$$

Since the last non-zero remainder is 5, that's the gcd.

2 Question 2

(10 points) Solve the system of linear equations shown:

$$x = 3 \pmod{301}$$
$$x = 5 \pmod{151}$$

You may not use a calculator/computer. Please show your work neatly and **show all steps**. When you are done, double-check your work.

Solution. We begin by doing the extended Euclidean algorithm to solve the linear Diophantine equation

$$301s + 151t = \gcd(301, 151).$$

I will represent the 'cards' as tuples, in LaTeX:

$$(301, s = 1, t = 0) = 1 \cdot (151, s = 0, t = 1) + (150, s = 1, t = -1)$$
$$(151, s = 0, t = 1) = 1 \cdot (150, s = 1, t = -1) + (1, s = -1, t = 2)$$

This gives $(s = -1, t = 2)$ as a solution to $301s + 151t = 1$ (it shows the gcd is 1 along the way).

It is also possible to solve this equation by inspection, since 301 is noticeably so close to two copies of 151. Therefore its ok if students simply point out that $t = 2$, $s = -1$ is an answer to this by inspection, with $\gcd(301, 151) = 1$.

It is useful to compute that

$$301 \cdot 151 = 45451.$$

To solve the Chinese Remainder Theorem problem, we set

$$\begin{aligned} x &\equiv 5 \cdot 301s + 3 \cdot 151t \pmod{45451} \\ &\equiv -5 \cdot 301 + 6 \cdot 151 \pmod{45451} \\ &\equiv -599 \pmod{45451} \\ &\equiv 44852 \pmod{45451} \end{aligned}$$

The answer is $x \equiv 44852 \pmod{45451}$.

3 Question 3

(10 points) What follows is an RSA message encrypted to your public key $(n, e) = (1211809, 13133)$. You have forgotten your private decryption exponent, but you do remember your primes p and q, which are

$$p = 1009, \quad q = 1201.$$

The message is 553962.

Decrypt the message. Hint: the plaintext is a nice roundish number.

Note: You may use Sage to do plain integer arithmetic (adding, multiplying) as well as plain modular arithmetic (multiplication, exponentiation, and/or inversion). **You must include any Sage code you used in your solution and indicate how/where you used it**. You may not use Sage's more complex functions (e.g., "euler_phi" is not allowed).

Please show your work neatly and **show all steps**. Missing steps may lose you credit.

Solution. In order to decrypt the message, you must re-create your decryption exponent. The decryption exponent is the inverse of the encryption exponent, modulo $\varphi(n)$. Therefore, you must compute a modular inverse.

Since $p = 1009, q = 1201$, we can compute

$$\varphi(n) = \varphi(pq) = (p-1)(q-1) = 1008 \cdot 1200 = 1209600.$$

Then, we have $e = 13133$, and we compute its inverse

$$d \equiv 13133^{-1} \equiv 369797 \pmod{1209600}.$$

Having recovered the decryption exponent d, we raise the message to that exponent:

$$553962^{369797} \equiv 100100 \pmod{1211809}.$$

4 Question 4

(10 points) Let $n = 22017$. You wish to factor n. Using the quadratic sieve, you obtain the following facts:

$$\begin{aligned}
149^2 &\equiv 2^3 \cdot 23^1 \pmod{n},\\
150^2 &\equiv 3^1 \cdot 7^1 \cdot 23^1 \pmod{n},\\
153^2 &\equiv 2^4 \cdot 3^1 \cdot 29^1 \pmod{n},\\
159^2 &\equiv 2^6 \cdot 3^1 \cdot 17^1 \pmod{n},\\
193^2 &\equiv 2^7 \cdot 7^1 \cdot 17^1 \pmod{n}.
\end{aligned}$$

Please explain how the Quadratic Sieve factoring process finds a non-trivial factor from this point onward.

Note: You may use Sage to compute integer arithmetic and gcds in this problem, but if you do, **you must include all Sage code you run as part of your solution**.

Solution. The first two and last two equations can be combined to give

$$(149 \cdot 150 \cdot 159 \cdot 193)^2 \equiv 2^{16} \cdot 3^2 \cdot 7^2 \cdot 17^2 \cdot 23^2 \pmod{n}.$$

Taking the gcd of $149 \cdot 150 \cdot 159 \cdot 193 - 2^8 \cdot 3 \cdot 7 \cdot 17 \cdot 23$ with n reveals a non-trivial factor of 537.

5 Question 5

(10 points) Let $n = 49141$. You know the following facts:

$$\begin{aligned} n - 1 &= 2^2 \cdot 12285 \\ 2^{12285} &\equiv 32527 \pmod{n} \\ 2^{2 \cdot 12285} &\equiv 49140 \pmod{n} \\ 2^{2^2 \cdot 12285} &\equiv 1 \pmod{n} \\ 3^{12285} &\equiv 627 \pmod{n} \\ 3^{2 \cdot 12285} &\equiv 1 \pmod{n} \\ 3^{2^2 \cdot 12285} &\equiv 1 \pmod{n} \end{aligned}$$

Decide if this information implies n is composite, or if the best conclusion one can make is that n is probably prime.

1. In either case, explain your answer with reference to either the "Basic Principle" or to Fermat's Little Theorem.

2. If n is composite determine a non-trivial factor.

Note: You may use Sage to compute integer arithmetic and gcds in this problem, but if you do, **you must include all Sage code you run as part of your solution**.

Solution. Consider the following two facts chosen from those above:

$$\begin{aligned} 3^{12285} &\equiv 627 \pmod{n} \\ 3^{2 \cdot 12285} &\equiv 1 \pmod{n} \end{aligned}$$

Since $627 \not\equiv \pm 1 \pmod{n}$, we have an instance of the Basic Principle, which says that if $x^2 \equiv y^2 \pmod{n}$ but $x \not\equiv \pm 1 \pmod{n}$, then $\gcd(x - y, n)$ is a nontrivial factor of n. Hence we take the non-trivial factor

$$\gcd(627 - 1, 49141) = 313.$$