North Carolina State University is a land-grant university and a constituent institution of The University of North Carolina

Department of Mathematics

NC STATE UNIVERSITY

MA 410 Theory of Numbers, final examination, Thursday, April 24, 2025
Prof. Erich Kaltofen <kaltofen@ncsu.edu>
https://users.cs.duke.edu/~elk27/courses/NumberTheory/Spring24/ (URL)

There are 6 problems on this exam divided into 10 sub-problems for a total of 48 points. Please take a photo/scan your solution of each problem done on paper (not necessarily the printed exam) and upload the problem on the Moodle course web page on https://wolfware.ncsu.edu.

By taking the exam, you agree that you will not consult with another human person about the solution. You can consult your notes/book/the Internet such as https://www.wolframalpha.com.

You have until 11am today, Thursday, April 24, to upload the photos/scans. I will be on Zoom from 8:30am-10:30am to answer questions about the exam.

Good luck!

MA 410 Number Theory Spring 2025 Final Exam Solution

Problem 1 (16 points)

(a, 4pts) True of false for Euler's totient function ϕ: for all $n \in \mathbb{Z}_{\geq 1}$: $\phi(2n) = \begin{cases} 2\phi(n) & \text{if } n \equiv 0 \pmod 2, \\ \phi(n) & \text{if } n \equiv 1 \pmod 2. \end{cases}$ Please explain.

True. If $n \equiv 0 \pmod 2$ *then* $n = 2^k m$ *with* $k \geq 1$ *and* $m \equiv 1 \pmod n$. *Then* $\phi(2n) = \phi(2^{k+1} m) = 2^k \phi(m)$ *and* $\phi(n) = 2^{k-1} \phi(m)$.
If $n \equiv 1 \pmod 2$ *then* $\phi(2n) = \phi(2)\phi(n) = \phi(n)$.

(b, 4pts) True or false: if $p \geq 5$ is a prime number with $p \equiv 5 \pmod{12}$ then $\left(\frac{3}{p}\right) = -1$. Please explain. [Hint: the Quadratic Reciprocity Law.]

True: $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = 1$ *because* $p \equiv 1 \pmod 4$. *Also* $\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$ *because* $p \equiv 2 \pmod 3$. *Therefore* $\left(\frac{3}{p}\right) = -1$.

(c, 4pts) True of false: Taher El Gamal's public key crytosystem as described in class is secure for smaller public keys than the RSA scheme, but additionally requires an algorithm for pseudo-random bit generation.

True. The discrete log for breaking El Gamal is harder than integer factoring for breaking RSA. But without random exponents for encryption, the scheme is subject to the lunchtime attack where an evesdropper has both their clear and their ciphertext.

(d, 4pts) Please compute $x, z \in \mathbb{Z}_{>0}$ such that $x^2 + 2025 = z^2$.

$2025 = 3^4 \cdot 5^2 = 3^2 \cdot 15^2$, *hence* $15^2(4^2 + 3^2) = 15^2 \cdot 5^2$*:* $x = 60, z = 75$.

$2025 = 45^2 = (7^2 - 2^2)^2, s = 7, t = 2, x = 2st = 28, z = s^2 + t^2 = 53$.

Smallest soltution: $(3 \cdot 2 \cdot 4 \cdot 1)^2 + (3 \cdot (4^2 - 1^2))^2 = 24^2 + 45^2 = (3 \cdot (4^2 + 1^2))^2 = 51^2$.

Problem 2 (5 points): The following is a trace of the computation of the Legendre symbol $\left(\frac{-1624}{2897}\right)$ using Jacobi's reciprocity law. Please fill in the blanks.

$$\underbrace{\left(\frac{-1624}{2897}\right)}_{=1} = \underbrace{\left(\frac{-1}{2897}\right)}_{1}\underbrace{\left(\frac{1624}{2897}\right)}_{1}; \quad \left(\frac{-1}{2897}\right) = 1 \quad (2897 \equiv 1 \pmod 4)$$

$$\underbrace{\left(\frac{1624}{2897}\right)}_{=1} = \underbrace{\left(\frac{8}{2897}\right)}_{1}\underbrace{\left(\frac{203}{2897}\right)}_{1}; \quad \left(\frac{2^3}{2897}\right) = 1 \quad (2897 \equiv 1 \pmod 8)$$

$$\underbrace{\left(\frac{203}{2897}\right)}_{=1}\underbrace{\left(\frac{2897}{203}\right)}_{1} = 1 \quad (2897 \equiv 1 \pmod 4) \quad 2897 \bmod 203 = 55;$$

$$\underbrace{\left(\frac{55}{203}\right)}_{=1}\underbrace{\left(\frac{203}{55}\right)}_{-1} = -1 \quad (55 \equiv 203 \equiv 3 \pmod 4) \quad 203 \bmod 55 = 38$$

$$\underbrace{\left(\frac{38}{55}\right)}_{=-1} = \underbrace{\left(\frac{2}{55}\right)}_{1}\underbrace{\left(\frac{19}{55}\right)}_{-1}; \quad \left(\frac{2}{55}\right) = 1 \quad (55 \equiv 7 \pmod 8)$$

$$\underbrace{\left(\frac{19}{55}\right)}_{=-1}\underbrace{\left(\frac{55}{19}\right)}_{1} = -1 \quad (19 \equiv 55 \equiv 3 \pmod 4) \quad 55 \bmod 19 = 17$$

$$\underbrace{\left(\frac{17}{19}\right)}_{=1}\underbrace{\left(\frac{19}{17}\right)}_{1} = 1 \quad (17 \equiv 1 \pmod 4) \quad \left(\frac{19}{17}\right) = \left(\frac{2}{17}\right) = 1 \quad (17 \equiv 1 \pmod 8) \quad \left(\frac{-1624}{2897}\right) = 1$$

Problem 3 (6 points): Using the Tonelli-Shanks algorithm from class, compute $b \in \mathbb{Z}_{233}$ such that $b^2 \equiv 29 \pmod{233}$. If you need a quadratic non-residue, please use the quadratic non-residue 17. You may use https://wolframalpha.com to compute the required powers and products modulo 233, but please show which modular powers and products you have computed.

$a^{(p-1)/4} = 29^{232/4} = 29^{58} \equiv 1 \pmod{233}$;
$29^{29} \equiv -1 \pmod{233}$, $29^{29} \cdot 17^{116} \equiv 1 \pmod{233}$;
$29^{30} \cdot 17^{116} \equiv 29 \pmod{233}$, $29^{15} \cdot 17^{58} \equiv 202 \pmod{233}$, $b = 202$, $202^2 \equiv 29 \pmod{233}$.

Problem 4 (10 points): Consider the following table of indices (discrete logarithms) for the prime number 29 with respect to the primitive root $g = 3$:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\text{ind}_3(a)$	0	17	1	6	10	18	8	23	2	27	5	7	26	25
a	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$\text{ind}_3(a)$	11	12	21	19	13	16	9	22	4	24	20	15	3	14

(a, 3pts) For the primitive root $g' = 2$ there is a constant residue $k \in \mathbb{Z}_{28}$ such that for all residues $a \in \mathbb{Z}_{29} \setminus \{0\}$ one has $\text{ind}_2(a) \equiv k \cdot \text{ind}_3(a) \pmod{28}$. Please compute k (using the above table) and show your work.

Set $a = 2$: $\text{ind}_2(2) = 1 \equiv k \cdot \text{ind}_3(2) \equiv 17 \cdot k \pmod{28}$; $k = (17^{-1} \bmod 28) = 5$.

(b, 7pts) Using the above table, please solve for $x \in \mathbb{Z}_{29}$, $y \in \mathbb{Z}_{29}$, and $z \in \mathbb{Z}_{29}$ the three congruences

$$3x^{27} \equiv 2 \pmod{29}, \quad 2y^4 \equiv 5 \pmod{29}, \quad 3z^7 \equiv 7 \pmod{29}.$$

Please give **all** solutions or indicate that there is none and show your work.

$27\text{ind}(x) + \text{ind}(3) \equiv \text{ind}(2) \pmod{28}$, $\text{ind}(x) \equiv (-1)(17-1) \equiv 12 \pmod{28}$, $x = 16$.

$4\text{ind}(y) + \text{ind}(2) \equiv \text{ind}(5) \pmod{28}$, $4\text{ind}(y) \equiv 10 - 17 \equiv 21 \pmod{28}$, but 4 does not divide 21, no solution.

$7\text{ind}(z) + \text{ind}(3) \equiv \text{ind}(7) \pmod{28}$, $7\text{ind}(z) \equiv 8 - 1 \equiv 7 \pmod{28}$, $\text{ind}(z) \equiv 1 \pmod{4}$, $\text{ind}(z) \equiv 1, 5, 9, 13, 17, 21, 25 \pmod{28}$, $z = 3, 11, 21, 19, 2, 17, 14$.

Problem 5 (5 points): Decrypt Alice's ciphertext (2008,601), (1087,22), (862,2397) that was encrypted by the el Gamal protocol with the public key $(g, p, g^s \bmod p) = (2, 2579, 387)$, where $387 = (2^{2000} \bmod 2579)$ and $s = 2000$ is Bob's secret. Here each pair in the ciphertext is $\left(2^{r_i}, \left(m_i \cdot 387^{r_i}\right) \bmod p\right)$ for $1 \leq i \leq 3$, where r_i are Alice's random choices and m_i are blocks of 2 letters as residues, where each pair of decimal digits corresponds to a letter: A=00, B=01, C=02,..., Z=25, blank space=26. [Hint: in wolfram|alpha $(a^e \bmod p)^{-1} \bmod p$ is `PowerMod[a,-e,p]`.]

$(2008^{-2000} \cdot 601) \bmod 2579 = 1314$*: "NO"*
$(1087^{-2000} \cdot 22) \bmod 2579 = 0304$*: "DE"*
$(862^{-2000} \cdot 2397) \bmod 2579 = 0011$*: "AL"*
"NODEAL"

Problem 6 (6 points) Please compute $x, y \in \mathbb{Z}_{>0}$ such that $x^4 - 2y^4 = z^2$. [Hint: if $s = \sqrt{2}s'$ and $z = s^2 - t^2$ then $(s^2-t^2)^2 + (2st)^2 = (\underbrace{2(s')^2 - t^2}_{z})^2 + 2(\underbrace{2s't}_{y^2})^2 = (s^2+t^2)^2 = (\underbrace{2(s')^2 + t^2}_{x^2})^2$.]

$s' = 2, t = 1, z = 7, y^2 = 4, x^2 = 9$: $3^4 - 2 \cdot 2^4 = 81 - 32 = 49 = 7^2$.

$s' = 2 \cdot 6^2, t = 7^2, y = 2 \cdot 6 \cdot 7 = 84, x^2 = 2(2 \cdot 6^2)^2 + 7^4 = 12769 = 113^2, x = 113,$
$113^4 - 2 \cdot 84^4 = 7967^2$.