4400-001 - SPRING 2022 - FINAL

Exam instructions. You have **two hours** to complete the exam. You may use any resource linked to from the class website, including the book and notes/whiteboards. You may also use your personal notes and your personal homeworks. You may use a calculator, including an online calculator or spreadsheet, to do computations, but you may not use a calculator that shows work (e.g., that carries out the Euclidean algorithm automatically and shows you the steps that it took). Your work should be your own, and you may not discuss the exam with anyone else until it is finished.

Name and signed statement of academic integrity (REQUIRED).
I certify that the work on this exam is my own, that I have not discussed any of the problems with my classmates or other people, and that I have followed the rules as explained in the exam instructions.
Name: Signature:

Exercise 1. True or False (30 points – 15 questions, 2 points each).
No justification is required for your true or false answer.

(1) $\sqrt{7}$ is a rational number. **True** / **False**

(2) Every non-zero rational number has a finite continued fraction expansion. **True** / **False**

(3) There is an integer solution to the following system of congruences. **True** / **False**

$$x \equiv 3 \mod 6 \text{ and } x \equiv 2 \mod 9$$

$\Rightarrow 3 \mid x$ $\Rightarrow 3 \nmid x$

(4) $|(\mathbb{Z}/555\mathbb{Z})^{\times}|$ is a prime number. **True** / **False**

$\phi(555) = \phi(5)\phi(111)$ so composite
>0 >0

(5) The last digit of 2023^{2023} is 7. **True** / **False**

$2023^{2023} \equiv 3^{2023} \mod 10$

$\phi(10) = 4$, $2023 = 505 \cdot 4 + 3$

so $3^{2023} \equiv 3^3 \mod 10$
$\equiv 27 \mod 10$
$\equiv 7 \mod 10$

(6) The polynomial $x^3 + x^2 + 2$ is irreducible/prime in $\mathbb{F}_7[x]$. **True** / **False**

x=2 is a root, so not irreducible.

(7) 2 is a primitive root in $\mathbb{Z}[i]/(3)$. **True** / **False**

$2^2 \equiv 1$, but $|(\mathbb{Z}[i]/(3))^\times| = 8$.

(8) RSA depends on the difficulty of discrete logarithm. **True** / **False**

Depends on difficulty of factoring and discrete logarithm — I accepted either answer since I realized when grading that this was misleading.

(9) $2^\ell - 1$ is always a prime number if ℓ is prime. **True** / **False**

Mersenne numbers

(10) -1 is a square mod 71. **True** / **False**

$71 \equiv 3 \mod 4$. is prime

(11) There are positive integers x and y such that $x^2 + y^2 = 71$. **True** / **False**

$71 \equiv 3 \bmod 4$ is prime

(12) $4^{50} \equiv -1 \mod 101$. **True** / **False**
Hint: 101 is prime; consider the explicit formula for the Legendre symbol.

$4^{50} = 4^{\frac{101-1}{2}} \equiv \left(\frac{4}{101}\right) = 1$ since $4 = 2^2$ is a square mod 101.

(13) There is an efficient way to check if $2^{2^n} + 1$ is prime. **True** / **False**

Pepin's test.

(14) $5 + 4i$ is a Gaussian prime/indecomposable. **True** / **False**

$N(5+4i) = 41$ is prime

(15) There are no square-pentagonal numbers. **True** / **False**

In Week 13 - Ex 1 we constructed lots!

Exercise 2. The Euclidean algorithm (30 points – 3 questions, 10 points each)
Show your work – an answer alone will not receive credit.

(1) Use the Euclidean algorithm to compute the multiplicative inverse of 24 in $\mathbb{F}_{71}$.

$71 = 2 \cdot 24 + 23$

$24 = 1 \cdot 23 + 1$

$1 = 24 - 1 \cdot 23$

$= 24 - (71 - 2 \cdot 24)$

$= \underline{\underline{3}} \cdot 24 - 71$

3 is the mult. inverse of 24 in $\mathbb{F}_{71}$

(2) Use the polynomial Euclidean algorithm to compute

$$\gcd(x^5 + x^3 + x^2 + 1,\ x^3 + 2x^2 + x + 2)$$

in $\mathbb{F}_7[x]$ (i.e. the polynomials are viewed as having coefficients in the field $\mathbb{F}_7$).

$x^2 - 2x + 4$

$x^3 + 2x^2 + x + 2 \,\overline{)\, x^5 + x^3 + x^2 + 1}$

$-(x^5 + 2x^4 + x^3 + 2x^2)$

$-2x^4 - x^2 + 1$

$-2x^4 - 4x^3 - 2x^2 - 4x$

$4x^3 + x^2 + 4x + 1$

$-(4x^3 + 8x^2 + 4x + 8)$ in $\mathbb{F}_7$!

$8x^2 = x^2$, $8 = 1$

$0.$

No remainder!

$x^3 + 2x^2 + x + 2$ divides ~~$x^2 - 2x + 4$~~ $x^5 + x^3 + x^2 + 1$ evenly

so gcd is

$x^3 + 2x^2 + x + 2$

(3) Use the Euclidean algorithm in $\mathbb{Z}[i]$ to compute the gcd of $30+i$ and ~~901~~ 53 in $\mathbb{Z}[i]$.

Corrected in class; was correct in electronic version on Zoom. Also added note $\frac{53}{901} = \frac{1}{17}$.

$$\frac{53}{30+i} = \frac{53(30-i)}{901} \text{ in } \mathbb{C}$$

$$= \frac{1}{17}(30-i)$$

$$= \frac{30}{17} - \frac{1}{17}i$$

Rounds to $2+0i$

so $53 = 2(30+i) + \underline{(-7-2i)}$ ← last nonzero remainder

~~30+i~~

$$\frac{30+i}{-7-2i} = \frac{(30+i)(-7+2i)}{53} = \frac{-212+53i}{53} = -4+i$$

so

$$30+i = (-4+i)(-7-2i) + 0$$

so gcd $= -7-2i$

If you wrote $\left(\frac{17}{589}\right)$, that doesn't work – Legendre symbol needs bottom ~~589~~ to be odd prime. If everything else was "right" I took off 2 points.

Exercise 3. Quadratic reciprocity (20 points – 2 questions, 10 points each)
Show your work – an answer alone will not receive credit.

(1) Is 17 a square modulo 589? *Hint: the prime factorization of 589 is* $19 \cdot 31$

* This was difficult, so I graded easy.

[illegible]

17 is a square mod 589 $\Leftrightarrow$ it is a square mod 19 and mod 31 (Chinese Remainder theorem)

$\left(\frac{17}{19}\right) = \left(\frac{19}{17}\right) = \left(\frac{2}{17}\right) = 1$ since $17 \equiv 1 \bmod 8$ ✓

$\left(\frac{17}{31}\right) = \left(\frac{31}{17}\right) = \left(\frac{14}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{7}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -1$

(3 not a square mod 7)

So $\boxed{\text{no}}$

(2) Is there a solution to $x^2 - 4x + 10 = 0$ in $\mathbb{F}_{131}$?

$x^2 - 4x + 10 = (x-2)^2 + 6$ $\quad (x-2)^2 + 6 = 0 \Leftrightarrow (x-2)^2 = -6$

So solution $\Leftrightarrow -6$ is a square in $\mathbb{F}_{131}$

$\left(\frac{6}{131}\right) = \left(\frac{3}{131}\right)\left(\frac{2}{131}\right)\left(\frac{-1}{131}\right)$ $\quad 131 = 128 + 3 = 16 \cdot 8 + 3 \equiv 3 \bmod 8$

$= \left(\frac{3}{131}\right) \cdot (-1) \cdot (-1)$

$= -\left(\frac{131}{3}\right)$ $\quad 131 = 129 + 2 = 43 \cdot 3 + 2 \equiv 2 \bmod 3$

$= -\left(\frac{2}{3}\right) = (-1)(-1)$

$= 1$

So $\boxed{\text{yes}}$

Exercise 4. Sums of two squares (10 points – 1 question)
Show your work – an answer alone will not receive credit.

Fact: The number 53 is prime and 2 is a primitive root in $\mathbb{F}_{53}$.
Starting from this fact, find positive integers x and y such that $x^2 + y^2 = 53$.

$2^{\frac{53-1}{4}} = 2^{13} \equiv 30 \mod 53.$

$30^2 \equiv -1 \mod 53.$

$30^2 + 1^2 = 901 = 17 \cdot 53$

Many did not use this fact to start, but the problem asks you to begin this way, and this is the method we learned in week 12 - Exercise 1.

Next – can either (1) realize that you computed gcd$(30+i, 53)$ in Exercise 2-3 and got $-7 + 2i$

$7^2 + 2^2 = 53.$

OR

do descent – $u \equiv 30 \mod 17$, $v \equiv 1 \mod 17$, $-\frac{17}{2} \leq u, v \leq \frac{17}{2}$

$\Rightarrow u = -4$, $v = 1$

$u - vi$

$(30 + i)(-4 - i) = (-119 - 34i)$

divide by 17

$-7 - 2i.$

$7^2 + 2^2 = 53$

Exercise 5. Pell's equations (10 points – 1 question)
Show your work – an answer alone will not receive credit.

Find two distinct pairs (x, y) of positive integers such that $x^2 - 5y^2 = 1$.
Hint: to find a first positive integer solution, try solving for x after plugging in small values of y. You won't be able to find the second one this way though!

Fist solution: $(9,4)$

$$(9+4\sqrt{5})^2 = 81+80+2\cdot 36\sqrt{5} = 161+72\sqrt{5}$$

$$N((9+4\sqrt{5})^2) = N(9+4\sqrt{5})^2 = 1^2 = 1$$

$$161^2 - 5\cdot 72^2$$

$$161^2 - 5\cdot(72)^2 = 1$$

$(9,4)$ and $(161, 72)$