# MATH 42 – PRACTICE FINAL

**Name:**______________________________________________________

FOR FULL CREDIT

SHOW ALL WORK

NO CALCULATORS

1. Find the GCD of 1234 and 357.

2. Find all solutions $x, y$ in $\mathbb{Z}$ to the linear diophantine equation $1234x + 357y = d$, where $d$ is the GCD of 1234 and 357.

3. Is 127 a square mod 617? Is 31 a square mod 617? (127, 617 and 31 are all prime.)

4. Mod which primes $p$ is 7 a square?

5. How many elements are there in $U_{1000}$?

6. Give an example of a function that is one-to-one, but not onto.

7. Give an example of a function that is onto, but not one-to-one.

8. Describe all solutions in $\mathbb{Z}$ to the equation

$$x^2 \equiv 2 \mod 119.$$

(Hint: $119 = 7 \cdot 17$.)

Here is a table with powers of 6 mod 41. Use it to solve the next two problems.

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $6^a$ | 6 | 36 | 11 | 25 | 27 | 39 | 29 | 10 | 19 | 32 | 28 | 4 | 24 | 21 | 3 | 18 | 26 | 33 | 34 | 40 |

| $a$ | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $6^a$ | 35 | 5 | 30 | 16 | 14 | 2 | 12 | 31 | 22 | 9 | 13 | 37 | 17 | 20 | 38 | 23 | 15 | 8 | 7 | 1 |

9. Use logarithms to find all inequivalent solutions to $40x^4 \equiv 1 \mod 41$.

10. What is the order of 18 mod 41? What is the order of 14 mod 41? Of $18 \cdot 14$?

11. Factor 3737 into primes in $\mathbb{Z}[i]$.

12. Write 3737 as the sum of two squares in two different ways.

13. Express $\sqrt{11}$ as a simple continued fraction.

14. Find two positive solutions to $x^2 - 11y^2 = 1$.

15. Give 4 examples of units in $\mathbb{Z}[\sqrt{11}]$, none of which may be 1 or $-1$.

16. Prove that for integers $a$ and $b$, any linear combination $ax+by$ with $x,y$ in $\mathbb{Z}$ is divisible by $d=(a,b)$. You may use the fact that the smallest natural number expressible in the form $ax+by$ is $d$.

17. Prove that for $z$ and $w$ in $\mathbb{Z}[i]$, $N(zw) = N(z)N(w)$. Use this to prove that if $N(z)$ and $N(w)$ are relatively prime in $\mathbb{Z}$, then $z$ and $w$ are relatively prime in $\mathbb{Z}[i]$.