MATH 42 – PRACTICE MIDTERM 2

Name:_____

FOR FULL CREDIT

SHOW ALL WORK

NO CALCULATORS

1. There is a marching band getting into certain configurations. When they line up in lines of 7, there is one person left over. When they line up in lines of 8, there are two people left over. When they line up in lines of 9, there is no one left over (that is, they are in a perfect 9-by-something rectangle). If you know that there are fewer than 500 people in the band, how many members do they have?

2. Compute $\left(\frac{3}{23}\right)$ using Euler's criterion and successive squaring.

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

3. Use logarithms to solve $25x^3 \equiv 9 \mod 41$.

4. What is the order of 18 mod 41? What is the order of 12 mod 41?

5. Can $4141 = 41 \cdot 101$ be written as a sum of two squares? If so, use factorization in $\mathbb{Z}[i]$ to find a representation $4141 = a^2 + b^2$ where a and b are integers.

6. In $\mathbb{Z}[i]$, $2+4i = 2(1+2i) = (1+i)(3+i)$. Does this show that $\mathbb{Z}[i]$ does not have unique prime factorization? Why or why not?

7. Prove that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

8. Give the algorithm for decryption in RSA cryptography. More precisely, we are given m and k with $(k, \varphi(m)) = 1$. The encoder, Alice, starts with the initial message x and sends Bob the encrypted message $b = x^k \mod m$. How does Bob recover x? Prove that your algorithm works.

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