Name: SOLUTIONS

Tuesday April 12, 2011
MATH 42 – Exam 2

For full credit, all work must be shown and clearly presented. No calculators.

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

1. In $\mathbb{Z}[i]$, $7+4i = (1+2i)(3-2i) = (2-i)(2+3i)$. Does this show that $\mathbb{Z}[i]$ does not have unique factorization? Why or why not? (5 points)

No, $\mathbb{Z}[i]$ still has unique factorization into primes.
$1+2i = (2-i)(+i)$ and $(3-2i) = (2+3i)(-i)$, so these factorizations are just off by units.

2. Factor 78 into primes in $\mathbb{Z}[i]$. (5 points)

$78 = 2 \cdot 3 \cdot 13$
$= (1+i)(1-i)\,3\,(2+3i)(2-3i)$.

3. Find all incongruent solutions mod 65 to

$$x^2 \equiv -1 \mod 65.$$

(10 points)

Note that $65 = 5 \cdot 13$.

Solve $x^2 \equiv -1 \mod 5$ and $x^2 \equiv -1 \mod 13$.

By inspection, $x \equiv \pm 2 \mod 5$ and $x \equiv \pm 5 \mod 13$.

We solve 4 systems of equations now:

① $x \equiv 2 \mod 5$
$x \equiv 5 \mod 13$

② $x \equiv 2 \mod 5$
$x \equiv -5 \mod 13$

③ $x \equiv -2 \mod 5$
$x \equiv 5 \mod 13$

④ $x \equiv -2 \mod 5$
$x \equiv -5 \mod 13$.

First find a s.t. $a \equiv 1 \mod 5$, $a \equiv 0 \mod 13$ and b s.t. $b \equiv 0 \mod 5$, $b \equiv 1 \mod 13$.

From guess + check, $a = 26$ works.

For b: $b = 5x = 13y + 1$.

$13 = 5 \cdot 2 + 3$
$5 = 3 \cdot 1 + 2$
$3 = 2 \cdot 1 + 1$
$2 = 1 \cdot 2 + 0$.

	2	1	1	2
0 1	2	3	5	13
1 0	1	1	2	5

$13 \cdot 2 - 5 \cdot 5 = 1$

So $b = -25$.

Solutions to: ① : $x \equiv 2(26) + 5(-25) \equiv 52 - 125 \equiv -73 \mod 65$

② : $x \equiv 2(26) + -5(-25) \equiv 52 + 125 \equiv 177 \mod 65$

③ : $x \equiv -2(26) + 5(-25) \equiv -52 - 125 \equiv -177 \mod 65$

④ : $x \equiv -2(26) - 5(-25) = -52 + 125 = 73 \mod 65$

So $\boxed{x = \pm 8, \pm 47 \mod 65}$

Here is a table of powers of 2 mod 37. Use it to solve the next two questions.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^a	2	4	8	16	32	27	17	34	31	25	13	26	15	30	23	9	18	36

a	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
2^a	35	33	29	21	5	10	20	3	6	12	24	11	22	7	14	28	19	1

4. Use logarithms to find all incongruent solutions mod 37

$$5x^6 \equiv 24 \mod 37.$$

(5 points)

$\log_2 5 + 6\log_2 x \equiv \log_2 24 \mod 36$

$23 + 6\log_2 x = 29 + 36k$ for some $k \in \mathbb{Z}$.

$6\log_2 x = 6 + 36k$

$\log_2 x = 1 + 6k = 1, 7, 13, 19, 25, 31, \ldots$

So $\boxed{x = 2, 17, 15, 35, 20, 22.}$

5. What is the order of 33^{25} in U_{37}? Of 25^{33}? Of $33^{25} \cdot 25^{33}$?

(5 points)

$33^{25} \equiv (2^{20})^{25} \equiv 2^{500} \equiv (2^{36})^{13} \cdot 2^{32} \equiv 2^{32} \mod 37.$

So the order is $\frac{36}{(36,32)} = \frac{36}{4} = \boxed{9}$.

$25^{33} \equiv (2^{10})^{33} \equiv 2^{330} \equiv (2^{36})^{9} \cdot 2^{6} \equiv 2^{6} \mod 37$

So the order is $\frac{36}{(36,6)} = \frac{36}{6} = \boxed{6}$.

$33^{25} \cdot 25^{33} \equiv 2^{32} \cdot 2^{6} \equiv 2^{38} \equiv 2^{2} \mod 37$

So the order is $\frac{36}{(36,2)} = \boxed{18}$

6. Compute $\left(\frac{6}{31}\right)$ using whatever method you choose. (5 points)

$\left(\frac{6}{31}\right) \equiv 6^{15} \bmod 31.$

$6^2 \equiv 36 \equiv 5 \bmod 31$

$6^4 \equiv 25 \equiv -6 \bmod 31$

$6^8 \equiv 36 \equiv 5 \bmod 31.$

So $6^{15} \equiv 5 \cdot (-6)(5)(6) \equiv (25)(-36) \equiv (-6)(-5) \equiv 30 \bmod 31.$

So $\left(\frac{6}{31}\right) = -1$

7. It is a fact that 13 is a square mod 131 and mod 173. Is -13 a square mod 131? Is -13 a square mod 173? (5 points)

131 is 3 mod 4 and 173 is 1 mod 4.

So $\left(\frac{-1}{131}\right) = -1$ and $\left(\frac{-1}{173}\right) = 1$

We're given $\left(\frac{13}{131}\right) = 1$ and $\left(\frac{13}{173}\right) = 1.$

So $\left(\frac{-13}{131}\right) = \left(\frac{-1}{131}\right)\left(\frac{13}{131}\right) = (-1)(1) = -1$ and $\left(\frac{-13}{173}\right) = \left(\frac{-1}{173}\right)\left(\frac{13}{173}\right) = 1.$

So -13 is not a square mod 131
and -13 is a square mod 173.

8. Again using the fact that 13 is a square mod 131 and mod 173, determine whether 52 is a square mod 131. Is 52 a square mod 173? (5 points)

Note: $52 = 4 \cdot 13.$

So $\left(\frac{52}{131}\right) = \left(\frac{4}{131}\right)\left(\frac{13}{131}\right) = 1 \cdot 1 = 1$ since $4 = 2^2$ is a square mod 131.

and $\left(\frac{52}{173}\right) = \left(\frac{4}{173}\right)\left(\frac{13}{173}\right) = 1 \cdot 1 = 1$ since $4 = 2^2$ is a square mod 173.

So 52 is a square mod 131 and also mod 173.

9. Prove that if u has order n in U_m, then u^k has order $\frac{n}{d}$ where $d = (k, n)$.
(10 points, 3 of which will be devoted to how well the proof is written)

Suppose $u^{kx} \equiv 1 \bmod m$. We'll show that $\frac{n}{d} \mid x$, which will imply that the smallest natural number x s.t. $(u^k)^x \equiv 1 \bmod m$ is $\frac{n}{d}$.

Now if $(u^k)^x \equiv 1 \bmod m$, we have $u^{kx} \equiv 1 \bmod m$.

Then $n \mid kx$ since n is the order of u.

In other words, there exists $l \in \mathbb{Z}$ s.t. $nl = kx$.

Then $\frac{n}{d} l = \frac{k}{d} x$, where $d = (k, n)$.

So we see that $\frac{n}{d} \mid \frac{k}{d} x$.

But $\left(\frac{n}{d}, \frac{k}{d}\right) = 1$ since d is the gcd of n and k

(and if $\left(\frac{n}{d}, \frac{k}{d}\right) = c \neq 1$, then $dc > d$ divides n and k).

Thus, by the fundamental theorem of arithmetic,

$\frac{n}{d} \mid x$.

Therefore, the order of u^k is $\frac{n}{d}$.

10. True/False: if true, prove the statement, if false, give a counterexample demonstrating the statement is false. Here, z, w are elements of $\mathbb{Z}[i]$. (5 points each)

I. If $N(z) = N(w)$, then z and w are associates (i.e. $w = \pm z$ or $w = \pm iz$).

II. If $N(z)$ and $N(w)$ are relatively prime in $\mathbb{Z}$, then z and w are relatively prime in $\mathbb{Z}[i]$.

III. If z and w are relatively prime in $\mathbb{Z}[i]$, then $N(z)$ and $N(w)$ are relatively prime in $\mathbb{Z}$.

I. False. For example, $2+i$ and $2-i$ are not associates, but $N(2+i) = N(2-i) = 5$.

II. True. We'll argue by contradiction. If z and w are not relatively prime in $\mathbb{Z}[i]$, they share a factor α, and α is not a unit.

So $z = \alpha z'$ and $w = \alpha w'$.

But then $N(z) = N(\alpha)\,N(z')$ and $N(w) = N(\alpha)\,N(w')$.

and we see that $N(\alpha)$ divides both $N(z)$ and $N(w)$.

Since $N(z)$ and $N(w)$ are relatively prime, their only common divisor is 1, but α not a unit $\Rightarrow N(\alpha) \neq 1$.

This is a contradiction, and z and w must be relatively prime in $\mathbb{Z}[i]$.

III. False. For example, $2+i$ and $2-i$ are relatively prime in $\mathbb{Z}[i]$ (they are both prime since their norms are prime).

But $N(2+i) = N(2-i) = 5$, so the norms are definitely not relatively prime.