MATH 42 – PRACTICE FINAL

Name: SOLUTIONS

FOR FULL CREDIT

SHOW ALL WORK

NO CALCULATORS

1. Find the GCD of 1234 and 357.

$$1234 = 357 \cdot 3 + 163$$
$$357 = 163 \cdot 2 + 31$$
$$163 = 31 \cdot 5 + 8$$
$$31 = 8 \cdot 3 + 7$$
$$8 = 7 \cdot 1 + \boxed{1}$$
$$7 = 1 \cdot 7 + 0$$

The GCD of 1234 and 357 is $\boxed{1}$.

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.

Use the magic box:

		3	2	5	3	1	7
0	1	3	7	38	121	159	1234
1	0	1	2	11	35	46	357

$$357 \cdot 159 - 1234 \cdot 46 = -1.$$

So $1234(46 + 357k) + 357(-159 - 1234k) = 1$

All solutions: $\boxed{\begin{array}{l} x = 46 + 357k \\ y = -159 - 1234k, \quad k \in \mathbb{Z}. \end{array}}$

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

$$\left(\frac{127}{617}\right) = \left(\frac{617}{127}\right) = \left(\frac{109}{127}\right) = \left(\frac{127}{109}\right) = \left(\frac{18}{109}\right) = \left(\frac{9}{109}\right)\left(\frac{2}{109}\right) = \left(\frac{2}{109}\right) = -1$$

So 127 is not a square mod 617 since $109 \equiv 5 \bmod 8$.

$$\left(\frac{31}{617}\right) = \left(\frac{617}{31}\right) = \left(\frac{28}{31}\right) = \left(\frac{4}{31}\right)\left(\frac{7}{31}\right) = \left(\frac{7}{31}\right) = -\left(\frac{31}{7}\right)$$

$$= -\left(\frac{3}{7}\right) = -(-1) = 1$$

So 31 is a square mod 617.

4. Mod which primes p is 7 a square?

If $p \equiv 1 \bmod 4$: $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 2, 4 \bmod 7 \\ -1 & \text{if } p \equiv 3, 5, 6 \bmod 7 \end{cases}$

If $p \equiv 3 \bmod 4$: $\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right) = \begin{cases} -1 & \text{if } p \equiv 1, 2, 4 \bmod 7 \\ 1 & \text{if } p \equiv 3, 5, 6 \bmod 7 \end{cases}$

So $\left(\frac{7}{p}\right) = 1$ if $p \equiv 1 \bmod 4$ and $p \equiv 1, 2$ or $4 \bmod 7$
OR $p \equiv 3 \bmod 4$ and $p \equiv 3, 5, 6 \bmod 7$

Put this together using Chinese remainder thm:
$a \equiv 1 \bmod 4,\ 0 \bmod 7 \longrightarrow a = -7$
$b \equiv 0 \bmod 4,\ 1 \bmod 7 \longrightarrow b = 8$ (by inspection).

So $\left(\frac{7}{p}\right) = 1$ if $\boxed{p \equiv 1, 9, 25, 3, 19, 27 \bmod 28}$.

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

There are $\varphi(1000)$ elements in $\mathcal{U}_{1000}$.

$$1000 = 10^3 = 2^3 \cdot 5^3, \text{ so } \varphi(1000) = \varphi(2^3)\varphi(5^3)$$
$$= (2^3-2^2)(5^3-5^2)$$
$$= 4 \cdot 100$$
$$= \boxed{400}.$$

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

There are many examples. Here is one:

$f(x) = 2x$ as a function from $\mathbb{Z}$ to $\mathbb{Z}$.

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

Again, there are many examples. Here is one:

$g(x) = x \bmod 5$ as a function from $\mathbb{Z}$ to $\mathbb{Z}_5$.

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

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

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

Mod 7: $x^2 \equiv 2 \mod 7$

$1^2 \equiv 1 \mod 7$, $2^2 \equiv 4 \mod 7$, $3^2 \equiv 2 \mod 7$, $4^2 \equiv 2 \mod 7$,

$5^2 \equiv 4 \mod 7$, $6^2 \equiv 1 \mod 7$,

so $x \equiv 3$ or $4 \mod 7$.

Mod 17: $x^2 \equiv 2 \mod 17$.

$6^2 \equiv 2 \mod 17$, so $x \equiv \pm 6 \mod 17$.

Now put it together with Chinese remainder theorem:

$a \equiv 1 \mod 7$, $0 \mod 17 \longrightarrow a = -34$ by inspection.

$b \equiv 0 \mod 7$, $1 \mod 17 \longrightarrow b = 35$ by inspection.

$x \equiv 3 \mod 7$ and $6 \mod 17$: $x \equiv 3(-34) + 6(35) \equiv 108 \mod 119$.

$x \equiv 3 \mod 7$ and $-6 \mod 17$: $x \equiv 3(-34) - 6(35) \equiv -312 \mod 119$.

$x \equiv 4 \mod 7$ and $6 \mod 17$: $x \equiv 4(-34) + 6(35) = 74 \mod 119$

$x \equiv 4 \mod 7$ and $-6 \mod 17$: $x \equiv 4(-34) - 6(35) \equiv -346 \mod 119$.

So $x = 108 + 119k$, $-312 + 119k$, $74 + 119k$ or $-346 + 119k$

for some $k \in \mathbb{Z}$.

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 $40x^4 \equiv 1 \mod 41$.

$$\log_6(40x^4) \equiv \log_6 1 \mod 40$$

$$\log_6 40 + 4\log_6 x \equiv 40 \mod 40$$

$$20 + 4\log_6 x = 40 + 40k \quad \text{some } k \in \mathbb{Z}$$

$$4\log_6 x = 20 + 40k$$

$$\log_6 x = 5 + 10k = 5, 15, 25, 35, 45, \ldots$$

So $\boxed{x \equiv 27, 3, 14, 38 \mod 41}$

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

$18 = 6^{16}$, so it has order $\dfrac{40}{(16,40)} = \dfrac{40}{8} = \boxed{5}$.

$14 = 6^{25}$, so it has order $\dfrac{40}{(25,40)} = \dfrac{40}{5} = \boxed{8}$.

$18 \cdot 14$ has order $\boxed{40}$ since $(5,8) = 1$.

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

$$3737 = 37 \cdot 101 = (36+1)(100+1).$$
$$= (6+i)(6-i)(10+i)(10-i).$$

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

$$(6+i)(10+i) = 59 + 16i$$
$$(6-i)(10+i) = 61 - 4i.$$

$$3737 = 59^2 + 16^2$$
$$= 61^2 + 4^2.$$

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

$$\sqrt{11} = 3 + (\sqrt{11}-3) = 3 + \cfrac{1}{\left(\cfrac{1}{\sqrt{11}-3}\right)} = 3 + \cfrac{1}{\cfrac{\sqrt{11}+3}{2}} = 3 + \cfrac{1}{3 + \cfrac{\sqrt{11}-3}{2}}$$

$$= 3 + \cfrac{1}{3 + \cfrac{1}{\cfrac{2}{\sqrt{11}-3}}} = 3 + \cfrac{1}{3 + \cfrac{1}{\cfrac{\cancel{2}(\sqrt{11}+3)}{\cancel{2}}}} = 3 + \cfrac{1}{3 + \cfrac{1}{3 + 3 + \cfrac{1}{3 + \cfrac{1}{3+\sqrt{11}}}}}$$

$$= 3 + \cfrac{1}{3 + \cfrac{1}{6 + \cfrac{1}{3 + \cfrac{1}{6 + \cdots}}}}$$

So $\sqrt{11} = [3, \overline{3, 6}]$.

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

		3	3	6
0	1	3	10	63
1	0	1	3	19
x^2-11y^2		-2	1	$\ldots$

$\boxed{\text{Solution 1: } x = 10,\ y = 3}$

$(10 + 3\sqrt{11})^2 = 100 + 99 + 60\sqrt{11}$, so $\boxed{\text{Solution 2: } x = 199,\ y = 60}$

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

$10 + 3\sqrt{11}$, $10 - 3\sqrt{11}$, $199 + 60\sqrt{11}$, $199 - 60\sqrt{11}$

are all units in $\mathbb{Z}[\sqrt{11}]$.

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.

Suppose $n=ax+by$. We want to show $d \mid n$.

Write $n=dq+r$, $q \in \mathbb{Z}$ and $r \in \mathbb{Z}$, $0 \le r < d$.

Then since d can be expressed as $d=ax_0+by_0$ for some $y_0, x_0 \in \mathbb{Z}$, we have

$$n=(ax_0+by_0)q+r = ax+by.$$

So $r = a(x-x_0q)+b(y-y_0q)$.

But d is the smallest natural number expressible as a linear combination of a and b, and $r<d$.

So r cannot be a natural number, and $r=0$.

Thus, $n=dq$ and $d \mid n$ by definition.

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 $\mathbb{Z}[i]$.

$$N(zw) = zw \cdot \overline{zw} \underset{(*)}{=} zw\bar{z}\bar{w} = z\bar{z}\,w\bar{w} = N(z)N(w)$$

$$\left(\overline{zw} = \bar{z}\bar{w} \text{ because } \overline{(a+bi)(c+di)} = (ac-bd)-(ad+bc)i = (a-bi)(c-di)\right).$$

If $N(z)$ and $N(w)$ are relatively prime, then z and w must be relatively prime because if z and w had a common factor α which is not a unit, then

$$z = \alpha z' \quad \text{and} \quad w = \alpha w'.$$

Then $N(z) = N(\alpha)N(z')$ and $N(w) = N(\alpha)N(w')$ and we see that $N(\alpha)$ is a common factor of $N(z)$ and $N(w)$.

But $N(\alpha) \neq 1$ since α is not a unit.

This contradicts the hypothesis that $(N(z), N(w)) = 1$, so we see that z and w cannot have a common factor other than a unit, and thus, z and w are relatively prime.