There are ten questions and the time allowed is 40 minutes. All working must be done on the quiz paper. Calculators will be supplied (no personal calculators may be used). I'll read and mark everything you write.
1. Find the gcd of \( f(x) = 6x^3 + 5x^2 + x - 4 \) and \( g(x) = 5x^2 - 4x + 6 \in \mathbb{Z}_7[x] \) using Euclid’s Algorithm.

**Solution**

\[
\begin{align*}
  f(x) &= 4xg(x) + 5x + 3 \\
  g(x) &= (x)(5x + 3) + 6 \\
  5x + 3 &= (2x + 4)6.
\end{align*}
\]

So the gcd is 6 (or 1, since it is only defined up to a unit factor.) Reading the array backwards:

\[
6 = g(x) - (x)(5x + 3)
= g(x) - (x)(f(x) - (4x)g(x))
= g(x)(1 + 4x^2) - xf(x).
\]

If you want to say the gcd is 1 multiply by \( 4^{-1} = 3 \) to get

\[
1 = g(x)(-1 - 4x^2) + xf(x).
\]

2. Find the gcd of \( 8 + 7i \) and \( 10 - 9i \in \mathbb{Z}[i] \), using Euclid’s Algorithm.

**Solution**

\[
\begin{align*}
  \frac{10 - 9i}{8 + 7i} &= \frac{17 - 142i}{113} \\
  &\approx -i, \text{ and so}
  10 - 9i &= (-i)(8 + 7i) + 3 - i. \text{ Similarly}
  8 + 7i &= (2 + 3i)(3 - i) - 1
  3 - i &= (-3 + i). - 1.
\end{align*}
\]

Hence the gcd \((8 + 7i, 10 - 9i) = -1 \in \mathbb{Z}[i] \) (or 1, up to unit factors)
3. Find the value of the Euler $\varphi$-function $\varphi(12240)$.

**Solution**

First $12240 = 16.9.5.17$ and so

$$\varphi(12240) = \varphi(16)\varphi(5)\varphi(9)\varphi(17)$$

$$= (16 - 8)(5 - 1)(9 - 3)(17 - 1)$$

$$= 8.4.6.16$$

$$= 3072.$$

4. Given that 109 and 113 can be written in the form $a^2 + b^2$, write 113.109 in the form $a^2 + b^2$ in two different ways.

**Solution**

\[
113 = 7^2 + 8^2
\]

\[
109 = 3^2 + 10^2, \text{ and so}
\]

\[
109.103 = (7^2 + 8^2)(3^2 + 10^2)
\]

\[
= (7.3 - 8.10)^2 + (7.10 + 8.3)^2
\]

\[
109.113 = 59^2 + 94^2. \text{ Similarly}
\]

\[
113 = 7^2 + 8^2
\]

\[
109 = 3^2 + (-10)^2, \text{ and so}
\]

\[
109.103 = (7^2 + 8^2)(3^2 + (-10)^2)
\]

\[
= (7.3 - 8.(-10))^2 + (7.(-10) + 8.3)^2
\]

\[
= 101^2 + 46^2.
\]
5. Given that my iPhone tells me that \( \frac{1}{107} = 0.00934\ 57943\ 92523 \). Of course you cannot rely on the last digit 3 which may be a 2 rounded up to an 3 by the phone.

(i) Use the given calculator to tell me the first correct 20 digits in the expansion.

(ii) What is the length of the periodic part of the decimal expansion?

**Solution**

Insert for example, 0.0.009345794392 into your calculator and multiply by 89. You get 52.999999 99999 44. This implies that to get an accurate remainder at that stage of the division, you need to add 56. Hence we use the calculator to find \( \frac{56}{107} = 0.52336\ 44859\ 81308 \). Hence \( \frac{1}{107} = 0.00934\ 57943\ 92523\ 36448\ 59813\ 08 \ldots \).

The period of the repeating part of the decimal is \( \text{ord}_{107}(10) \), which is a divisor of 106, that is, it is either 1, 2, 53 or 106. It turns out that \( \text{ord}_{107}(10) = 53 \). You can either do this by calculating \( \text{ord}_{107}(10) \) or by finding the decimal expansion of \( \frac{1}{107} \).

\[
\begin{align*}
10^2 &\equiv -7 \pmod{107} & 10^{16} &\equiv 69 \pmod{107} \\
10^4 &\equiv 49 \pmod{107} & 10^{32} &\equiv 53 \pmod{107} \\
10^8 &\equiv 47 \pmod{107} & 10^{53} &\equiv 10^{32}\cdot10^{16}\cdot10^{4}\cdot10 \pmod{107}
\end{align*}
\]

Hence \( 10^{53} \equiv 1 \pmod{107} \) and the decimal repeats after 53 steps. The full decimal expansion is:

\[
\frac{1}{107} = 0.00934\ 57943\ 92523\ 36448\ 59813\ 08411\ 21495\ 32710\ 28037\ 38317\ 757|00934\ldots
\]

6. Apply the Method of Gauss’s Lemma to calculate \( \left( \frac{5}{73} \right) \).

**Solution**

\[
\begin{array}{cccccccccccccccc}
1 & 2 & 3 & \ldots & 7 & 8 & 9 & \ldots & 13 & 14 & 15 & \ldots & 21 & 22 & 23 & \ldots & 29 & 30 & 31 & \ldots & 35 & 36 \\
5 & 10 & 15 & \ldots & 35 & -33 & -28 & \ldots & -8 & -3 & 2 & \ldots & 32 & -36 & -31 & \ldots & -1 & 4 & 9 & \ldots & 29 & 34
\end{array}
\]

Hence \( \mu_{73}(5) = 15 \), and so \( \left( \frac{5}{73} \right) = (-1)^{15} = -1 \) and 5 is a non-square modulo 73.
7. Use the Method of Descent to write the prime 5153 in the form $a^2 + b^2$, given that $\sqrt{-1} = 4926 \in \mathbb{Z}_{5153}$.

**Solution**

First we use $\sqrt{-1} = 5153 - 4926 = 227$ to shorten the work. We get $227^2 + 1^2 = 10.5153$.

Hence we have

$$227^2 + 1^2 = 5153.10$$

$$(-3)^2 + (-1)^2 = 10,$$

and multiplying

$$5153.10^2 = (227^2 + 1^2)((-3)^2 + (-1)^2)$$

$$= (227.(-3) - 1.(-1))^2 + (227.(-1) + 1.(-3))^2$$

$$= 680^2 + 230^2,$$

and dividing by $10^2$

$$5153 = 68^2 + 23^2.$$ 

8. Show that $\mathbb{Z}_{11}[x]_{x^3 + 2x + 4}$ is a field but that $\mathbb{Z}_{11}[x]_{x^3 + 2x + 1}$ is not a field.

**Solution**

If $f(x) = x^3 + 2x + 4$ has any proper factors, it must have a linear factor, that is, it will then have a root. Check:

$$f(0) = 4 \quad f(-5) = 10$$
$$f(1) = 7 \quad f(-4) = 9$$
$$f(2) = 3 \quad f(-3) = 4$$
$$f(3) = 4 \quad f(-2) = 3$$
$$f(4) = 10 \quad f(-1) = 1$$
$$f(5) = 7$$

Hence $f(x)$ has no linear factor and so is a prime. Thus $\mathbb{Z}_{11}[x]_{x^3 + 2x + 4}$ is a field.

Now consider $g(x) = x^3 + 2x + 1$ in the same way.

$$g(0) = 1 \quad g(-5) = 9$$
$$g(1) = 4 \quad g(-4) = 6$$
$$g(2) = 2 \quad g(-3) = 1$$
$$g(3) = 1 \quad g(-2) = 0$$
$$g(4) = 7 \quad g(-1) = 9$$
$$g(5) = 4$$

Hence $g(x) = (x + 2)(x^2 - 2x + 6)$ and is not prime. Hence both $x + 2$ and $x^2 - 2x + 6$ are zero divisors in $\mathbb{Z}_7[x]_{x^3 + x + 2}$ and so it cannot be a field (which has no zero divisors).
9. Solve the system of congruences

\[ x \equiv 1 \pmod{13} \]
\[ x \equiv 4 \pmod{9} \]
\[ x \equiv 6 \pmod{14}. \]

**Solution**

Solving the first congruence we have \( x = 1 + 13k \) and we then need \( 1 + 13k \equiv 4 \pmod{9} \). That is, \( 4k \equiv 3 \pmod{9} \) and dividing by 4 (mod 9) we have \( k \equiv 3 \pmod{9} \) and \( k = 3 + 9\ell \). Hence \( x = 1 + 13(3 + 9\ell) = 40 + 13.9\ell \).

Finally \( 40 + 13.9\ell \equiv 6 \pmod{14} \). Hence \( 13.9\ell \equiv 8 \pmod{14} \) and \( 13.9 = 117 \equiv 5 \pmod{14} \) and so \( \ell \equiv 10 \pmod{14} \) and \( \ell = 10 + 14m \) for some integer \( m \). Hence

\[ x = 40 + 13.9(10 + 14m) = 1210 + 13.9.14m. \]

This completes the proof.

10. Apply the Law of Quadratic Reciprocity to calculate \( \left(\frac{2677}{3511}\right) \). Both 2677 and 3511 are primes.

**Solution**

\[ \left(\frac{2677}{3511}\right) = \left(\frac{3511}{2677}\right), \text{ since } 2677 \equiv 1 \pmod{4} \]

\[ = \left(\frac{834}{2677}\right) \]

\[ = \left(\frac{2.3.139}{2677}\right) \]

\[ \left(\frac{2}{2677}\right) \left(\frac{3}{2677}\right) \left(\frac{139}{2677}\right). \]

You have to check somehow that 139 is or is not a prime. It is. To do that you need to divide by all primes \( \leq \sqrt{139} \).

Now \( \left(\frac{2}{2677}\right) = -1 \) since \( 2677 \equiv 5 \pmod{8} \).

Also

\[ \left(\frac{3}{2677}\right) = \left(\frac{2677}{3}\right), \text{ since } 2677 \equiv 1 \pmod{4} \]

\[ = \left(\frac{1}{3}\right) \]

\[ = 1, \]
Finally

\[
\left(\frac{139}{2677}\right) = \left(\frac{2677}{139}\right), \text{ since } 2677 \equiv 1 \pmod{4}
\]

\[= \left(\frac{36}{139}\right)\]

\[= 1, \text{ since } 36 \text{ is a square.}\]

Hence \(\left(\frac{2677}{3511}\right) = (-1).1.1 = -1\) and 2677 is a non-square modulo 3511.