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 \( f(x) = 5x^3 + 2x^2 + x - 4 \) and \( g(x) = 4x^2 - 4x + 6 \in \mathbb{Z}_7[x] \) using Euclid’s Algorithm.

**Solution**

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

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

Reading the array backwards:

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

If you want to say the gcd is 1 multiply by \(-1\) to get

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

2. Find the gcd of \( 7 + 5i \) and \( 8 - 7i \in \mathbb{Z}[i] \), using Euclid’s Algorithm.

**Solution**

\[
\begin{align*}
  \frac{8 - 7i}{7 + 5i} &= \frac{21 - 89i}{74} \\
  &\approx -i, \text{ and so} \\
  8 - 7i &= (-i)(7 + 5i) + 3. \text{ Similarly} \\
  7 + 5i &= (2 + 2i)3 + 1 - i \\
  3 &= (2 + 2i)(1 - i) - 1 \\
  1 - i &= (-1 + i)(-1).
\end{align*}
\]

Hence the gcd \((8 - 7i, 7 + 5i) = -1 \in \mathbb{Z}[i]. \) (OR again you can say it is 1 up to a unit factor.)
3. Find the value of the Euler $\varphi$– function $\varphi(12340)$.

**Solution**

First $12340 = 4 \cdot 5 \cdot 617$. Now $617$ is not divisible by any prime $\leq \sqrt{617} = 24.83\ldots$ and so is a prime. *(You have to make some effort to check that 617 is a prime - otherwise the answer will be wrong.)*

Hence

\[
\varphi(12340) = \varphi(4)\varphi(5)\varphi(617) = (4 - 2)(5 - 1)(617 - 1) = 2 \cdot 4 \cdot 616 = 4928.
\]

4. Given that 97 and 89 can be written in the form $a^2 + b^2$, write 97.89 in the form $a^2 + b^2$ in two different ways.

**Solution**

\[
\begin{align*}
97 &= 4^2 + 9^2 \\
89 &= 5^2 + 8^2, \text{ and so} \\
89.97 &= (4^2 + 9^2)(5^2 + 8^2) \\
&= (4.5 - 9.8)^2 + (4.8 + 9.5)^2 \\
&= 52^2 + 77^2. \text{ Similarly} \\
97 &= 4^2 + 9^2 \\
89 &= 5^2 + (-8)^2 \\
89.97 &= (4^2 + 9^2)(5^2 + (-8)^2) \\
&= (4.5 - 9(-8))^2 + (4(-8) + 9.5)^2 \\
89.97 &= 92^2 + 13^2.
\end{align*}
\]
5. Given that my iPhone tells me that \( \frac{1}{113} = 0.00884\ 95575\ 22124 \): Of course you cannot rely on the last digit 4 which may be a 3 rounded up to a 4 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, 0.9557522 into your calculator and multiply by 113. You get 107.9999986. This implies that to get an accurate remainder at that stage of the division, you need to add 14. Hence we use the calculator to find \( \frac{14}{113} = 0.12389\ 38053\ 09734 \). It is clear that the phone has rounded \( \frac{1}{113} = 0.00884\ 95575\ 22123\ 89380 \ldots \); to \( \frac{1}{113} = 0.00884\ 95575\ 22124 \), thinking that we weren’t interested in that last digit’s exact value. Thus it is clear that \( \frac{1}{113} = 0.00884\ 95575\ 22123\ 89380\ 53097\ 34 \ldots \).

The period of the repeating part of the decimal is \( \text{ord}_{113}(10) \), which is a divisor of 112 = 16\( \cdot \)7, that is it is one of 1, 2, 4, 7, 8, 14, 16, 28, 56, 112. It turns out that \( \text{ord}_{113}(10) = 112 \). You can do this by calculating \( \text{ord}_{113}(10) \) or by writing out the decimal expansion. If it is bigger than 56, it must be 112.

\[
\begin{align*}
10^2 &\equiv -13 \pmod{113} & 10^{16} &\equiv 106 \pmod{113} \\
10^4 &\equiv 56 \pmod{113} & 10^{28} &\equiv 15 \pmod{113} \\
10^7 &\equiv 65 \pmod{113} & 10^{56} &\equiv -1 \pmod{113} \\
10^8 &\equiv 85 \pmod{113} & 10^{112} &\equiv 1 \pmod{113} \\
10^{14} &\equiv 44 \pmod{113}
\end{align*}
\]

and so \( \text{ord}_{113}(10) = 112 \) and \( \frac{1}{113} \) has decimal expansion with periodic part of length 112.

The full decimal expansion of \( \frac{1}{113} \) is:

\[
\begin{align*}
0. & 00884\ 95575\ 22123\ 89380\ 53097\ 34513 \\
& 27433\ 62831\ 85840\ 70796\ 46017\ 69911 \\
& 50442\ 47787\ 61061\ 94690\ 26548\ 67256 \\
& 63716\ 81415\ 92920\ 35398\ 23000\ 88 \ldots
\end{align*}
\]

Note that the cycle repeats after 112 steps. Note also the symmetry about the 56th integer, namely 6\ 9911 \ldots .

6. Apply the Method of Gauss’s Lemma to calculate \( \left( \frac{5}{67} \right) \).

**Solution**

\[
\begin{array}{cccccccccccccccccccccccc}
1 & 2 & 3 & \ldots & 6 & 7 & 8 & \ldots & 13 & 14 & 15 & \ldots & 20 & 21 & 22 & \ldots & 26 & 27 & 28 & \ldots & 32 & 33 \\
5 & 10 & 15 & \ldots & 30 & -32 & -27 & \ldots & -2 & 3 & 8 & \ldots & 33 & -29 & -24 & \ldots & -4 & 1 & 6 & \ldots & 26 & 31
\end{array}
\]

Hence \( \mu_{67}(5) = 13 \), and so \( \left( \frac{5}{67} \right) = (-1)^{13} = -1 \) and 5 is a non-square modulo 67.
7. Use the Method of Descent to write the prime 1613 in the form \(a^2 + b^2\), given that \(\sqrt{-1} = 1486 \in \mathbb{Z}_{1613}\).

**Solution**

First we use \(\sqrt{-1} = 1613 - 1486 = 127\) to shorten the work. We get \(127^2 + 1^2 = 10.1613\). Read this equation modulo 10 to get \((-3)^2 + 1^2 = 10\).

Hence we have

\[
127^2 + 1^2 = 1613.10
\]

\[
(-3)^2 + (-1)^2 = 10, \text{ and multiplying}
\]

\[
977.10^2 = (127^2 + 1^2)((-3)^2 + (-1)^2)
\]

\[
= (127.(-3) - 1.(-1))^2 + (127.(-1) + 1.(-3))^2
\]

\[
= 380^2 + 130^2, \text{ and dividing by } 10^2
\]

\[
1613 = 38^2 + 13^2.
\]

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

**Solution**

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

\[
\begin{align*}
    f(0) & = 4 & f(-5) & = 6 \\
    f(1) & = 6 & f(-4) & = 9 \\
    f(2) & = 3 & f(-3) & = 4 \\
    f(3) & = 1 & f(-2) & = 5 \\
    f(4) & = 6 & f(-1) & = 2 \\
    f(5) & = 2
\end{align*}
\]

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

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

\[
\begin{align*}
    g(0) & = 2 \\
    g(1) & = 4 \\
    g(2) & = 1 \\
    g(4) & = 4 \\
    g(5) & = 0.
\end{align*}
\]

Hence \(g(x) = (x - 5)(x^2 + 5x + 4)\) and is not prime. Hence both \(x - 5\) and \(x^2 - 5x + 4\) are zero divisors in \(\mathbb{Z}_{11}[x]_[x^3+x+2]\) and so it cannot be a field (which has no zero divisors).

As it happens \(x^3 + x + 2 = (x - 5)(x + 1)(x + 4)\), and so \(x - 5, x + 1\) and \(x + 4\) are zero divisors. And of course there are others. This is just an accident. One zero divisor is enough to ensure that it’s not a field.
9. Solve the system of congruences

\[ x \equiv 3 \pmod{13} \]
\[ x \equiv 5 \pmod{9} \]
\[ x \equiv -6 \pmod{14}. \]

**Solution**

Solving the first congruence we have \( x = 3 + 13k \) and we then need \( 3 + 13k \equiv 5 \pmod{9} \). That is \( 4k \equiv 2 \pmod{9} \) and dividing by 4 (mod 9) we have \( k \equiv 5 \pmod{9} \) and \( k = 5 + 9\ell \). Hence \( x = 3 + 13(5 + 9\ell) = 68 + 13.9\ell \).

Finally \( 68 + 13.9\ell \equiv -6 \pmod{14} \). Hence \( 13.9\ell \equiv 10 \pmod{14} \) and \( 13.9 = 117 \equiv 5 \pmod{14} \) and so \( \ell \equiv 2 \pmod{14} \) and \( x\ell = 2 + 14m \) for some integer \( m \). Hence

\[ x = 68 + 13.9(2 + 14m) = 302 + 13.9.14m. \]

This completes the proof.

10. Apply the Law of Quadratic Reciprocity to calculate \( \left( \frac{1973}{3727} \right) \). Both 1973 and 3727 are primes.

**Solution**

\[ \left( \frac{1973}{3727} \right) = \left( \frac{3727}{1973} \right), \text{ since } 1973 \equiv 1 \pmod{4} \]
\[ = \left( \frac{-219}{1973} \right) \]
\[ = \left( \frac{-3.73}{1973} \right) \]
\[ = \left( \frac{-1}{1973} \right) \left( \frac{3}{1973} \right) \left( \frac{73}{1973} \right). \]

Now \( \left( \frac{-1}{1973} \right) = 1 \) since \( 1973 \equiv 1 \pmod{4} \).

Also

\[ \left( \frac{3}{1973} \right) = \left( \frac{1973}{3} \right), \text{ since } 1973 \equiv 1 \pmod{4} \]
\[ = \left( \frac{2}{3} \right) \]
\[ = -1. \]

Finally

\[ \left( \frac{73}{1973} \right) = \left( \frac{1973}{73} \right), \text{ since } 1973 \equiv 1 \pmod{4} \]
\[ = \left( \frac{2}{73} \right) \]
\[ = 1, \text{ since } 73 \equiv 1 \pmod{8}. \]

Hence \( \left( \frac{1973}{3727} \right) = 1 \). \( -1.1 = -1 \) and 1973 is a non-square modulo 3727.