1. (a) Show that \( x^{40} \equiv 1 \pmod{100} \), for every integer \( x \) with \( (x, 100) = 1 \). (Hint: First calculate \( x^4 \pmod{10} \).)

(b) Is this true if \( (x, 100) \neq 1 \)?

**Solution**

(a) If \( x \equiv 1, 3, 7, 9 \pmod{10} \), then it is easy to show that \( x^4 \equiv 1 \pmod{10} \).

But then \( x^4 = 1 + 10k \), for some integer \( k \) and so

\[
x^{40} = (1 + 10k)^{10} = 1 + 100k + \binom{10}{2}100k^2 + \binom{10}{3}1000k^3 + \ldots \equiv 1 \pmod{100},
\]

since it is easy to see that 100 divides every term occurring in the expansion of \( (1 + 10k)^{10} \).

(b) If \( (x, 100) \neq 1 \), then \( x \) is either divisible by 2 or by 5. In any case raising \( x \) to any power always produces an even integer or one which ends in 5.

It is clear that such an integer cannot end in 1.

2. Decide if the equation \( 317x + 419y = 21 \) can be solved in \( \mathbb{Z} \). If it can, solve it.

**Solution**

\[
\begin{align*}
419 &= 1.317 + 102 \\
317 &= 3.102 + 11 \\
102 &= 9.11 + 3 \\
11 &= 3.3 + 2 \\
3 &= 1.2 + 1 \\
2 &= 2.1.
\end{align*}
\]

So the \( \text{gcd}(419, 317) = 1 \), and 1 divides 21. Hence a solution exists.

This time we’ll apply a Magic Table:

\[
\begin{array}{cccccccc}
1 & 3 & 9 & 3 & 1 & 2 \\
0 & 1 & 1 & 4 & 37 & 115 & 152 & 419. \\
1 & 0 & 1 & 3 & 28 & 87 & 115 & 317
\end{array}
\]

Hence

\[
317.152 - 115.419 = -1
\]

and so, multiplying by \(-21\), we get

\[
317.(-3192) + 419.(2415) = 21.
\]
Every solution can be written in the form
\[ x = -3192 + 419k, \quad y = 2415 - 317k, \]
where \( k \) is any integer.

3. Evaluate the following fractions:
\[ \frac{1}{3}, \quad 1 + \frac{1}{3}, \quad 1 + \frac{1}{3 + \frac{1}{9}}, \quad 1 + \frac{1}{3 + \frac{1}{9 + \frac{1}{3}}}, \]
\[ 1 + \frac{1}{3 + \frac{1}{9 + \frac{1}{3 + \frac{1}{3 + \frac{1}{1}}}}}, \quad 1 + \frac{1}{3 + \frac{1}{9 + \frac{1}{3 + \frac{1}{3 + \frac{1}{1 + \frac{1}{2}}}}}}. \]

**Solution**
Use the Magic Table.

\[
\begin{array}{ccccccccc}
1 & 3 & 9 & 3 & 1 & 2 & 0 & 1 & 1 & 4 & 37 & 115 & 152 & 419 \\
& 1 & 0 & 1 & 3 & 28 & 87 & 115 & 317
\end{array}
\]

The required values are thus
\[ 1, \quad 4, \quad 37, \quad 115, \quad 152, \quad 419. \]

4. (a) Show that \( 11 + 17i \) is divisible by \( 1 + i \) in \( \mathbb{Z}[i] \) and so \( 11 + 17i \) is not a prime in \( \mathbb{Z}[i] \).
(b) Show that \( a + ib \) is not a prime in \( \mathbb{Z}[i] \) if \( a \) and \( b \) are either both even or both odd.

**Solution**
(a) \[ 11 + 17i = (1 + i)(14 + 3i). \]
(b) If \( a \) and \( b \) are both even, then \( a + bi \) is obviously a multiple of 2 and so it’s not a prime. If \( a \) and \( b \) are both odd,
\[
\frac{a + ib}{1 + i} = \frac{(a + ib)(1 - i)}{(1 + i)(1 - i)}
= \frac{a + b + i(\bar{a} + \bar{b})}{2}
= \frac{a + b}{2} + i\frac{\bar{a} + \bar{b}}{2}
\in \mathbb{Z}[i],
\]

since both \( a + b \) and \( a - b \) are integers if \( a \) and \( b \) are both odd. This completes the proof.

5. Use the Euclidean Algorithm in \( \mathbb{Z}_7[x] \) to calculate the greatest common divisor \( d(x) \) of
\[ f(x) = 3x^3 - 2x^2 + 2x - 4 \quad \text{and} \quad g(x) = 5x^2 + 3x - 2 \]
and write \( d(x) \) in the form \( a(x)f(x) + b(x)g(x) \), with \( a(x), b(x) \in \mathbb{Z}_7[x] \), in two different ways.

**Solution**
3x^3 - 2x^2 + 2x - 4 = (2x - 3)(5x^2 + 3x - 2) + x - 3
5x^2 + 3x - 2 = (5x + 4)(x - 3) + 3
x - 3 = (5(x - 3)) 3
= (5x - 1)3.

Hence the greatest common divisor \( d(x) = 3 \), the last non-zero remainder. (Since the gcd is only defined up to unit factors, we might as well say that the gcd is 1.) Reading the Euclidean array backwards, we have

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

Hence

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

A second way to write 6 or 1 in terms of \( f(x) \) and \( g(x) \) is as follows:

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

Of course this can be done in infinitely many ways.

6. List all the primes of degree at most 3 in \( \mathbb{Z}_2[x] \) and \( \mathbb{Z}_3[x] \).

**Solution**

\( \mathbb{Z}_2[x] \): \( x, x + 1, x^2 + x + 1, x^3 + x + 1, x^3 + x^2 + 1 \).

Verify that the other polynomials of degree \( \leq 3 \) all are composite in \( \mathbb{Z}_2[x] \).

\( x^2 + 1 = (x + 1)^2, x^3 + 1 = (x + 1)(x^2 + x + 1), x^3 + x^2 + x + 1 = (x + 1)^3 \).

\( \mathbb{Z}_3[x] \):

<table>
<thead>
<tr>
<th>( x )</th>
<th>( x + 1 )</th>
<th>( x^2 + x + 2 )</th>
<th>( x^2 + 2x + 2 )</th>
<th>( x^3 + 2x + 1 )</th>
<th>( x^3 + 2x + 2 )</th>
<th>( x^3 + x^2 + 2 )</th>
<th>( x^3 + x^2 + x + 2 )</th>
<th>( x^3 + x^2 + 2x + 1 )</th>
<th>( x^3 + 2x^2 + x + 1 )</th>
<th>( x^3 + 2x^2 + x + 2 )</th>
</tr>
</thead>
</table>

Hint:

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

7. Consider the following two steps in the Euclidean algorithm applied to \( a, b \) with \( a > b > 0 \).

\[
a = bq_1 + r_1 \quad 0 \leq r_1 < b \\
b = r_1q_2 + r_2 \quad 0 \leq r_2 < r_1
\]
(a) Show that if \( r_1 \leq \frac{1}{2} b \), then \( r_2 < \frac{1}{2} b \).

(b) Show that if \( r_1 > \frac{1}{2} b \), then \( q_2 = 1 \) and so \( r_2 < \frac{1}{2} b \).

(c) Hence show that \( r_{2k} < \frac{1}{2^k} b \) for each \( k \) and so \( r_{2k} = 0 \) when \( 2k > \frac{2 \ln b}{\ln 2} > 2.88 \ln b \).

(Hence the algorithm terminates in less than \( 2.89 \ln b \) steps. So Euclid’s Algorithm for two numbers say with 100 digits (that is around \( 10^{100} \)) will terminate in at most \( 2.89 \ln(10^{100}) = 2.89 \times 100 \ln 10 \leq 665 \) divisions.)

Solution

\[
a = bq_1 + r_1, \quad 0 \leq r_1 < b \\
b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1
\]

If \( r_1 \leq \frac{1}{2} b \), then \( r_2 < r_1 \leq \frac{1}{2} b \).

If \( r_1 > \frac{1}{2} b \), then \( r_1q_2 \geq 2r_1 > b \), if \( q_2 \geq 2 \). Since \( r_1q_2 = b - r_1 \leq b \), we must have \( q_2 = 1 \).

But then \( b = r_1 + r_2 \) and so \( r_2 = b - r_1 < b - \frac{1}{2} b = \frac{1}{2} b \).

Finally the Euclidean Algorithm has the form

\[
a = bq_1 + r_1, \quad 0 \leq r_1 < b \\
b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1 \\
r_1 = r_2q_3 + r_3, \quad 0 \leq r_3 < r_2 \\
r_2 = r_3q_4 + r_4, \quad 0 \leq r_4 < r_3 \\
\vdots \\
r_{n-2} = r_{n-1}q_n + r_n, \quad 0 \leq r_n < r_{n-1} \\
r_{n-1} = r_nq_{n+1}
\]

Now apply part (b) to the first two equations. We get \( r_2 < \frac{1}{2} b \), while applying it to the third and fourth equations we get \( r_4 < \frac{1}{2} r_2 \).

Thus \( r_4 < \frac{1}{2^2} b \). Similarly, \( r_{2k} < \frac{1}{2^k} b \).

If \( k \) is such that \( \frac{1}{2^k} b < 1 \), then \( r_{2k} = 0 \), since \( r_{2k} \geq 0 \) and is an integer.

So Euclid’s Algorithm terminates after \( 2k \) steps where \( \frac{1}{2^k} b < 1 \). (It may terminate before this!)

Now \( \frac{1}{2^k} b < 1 \) when \( b < 2^k \), that is when \( \ln b < k \ln 2 \).

Hence \( r_{2k} = 0 \), when \( 2k > \frac{2 \ln b}{\ln 2} = 2.88539 \ldots \ln b \).