Preparatory problems for AMSI course
Prime numbers in arithmetic progressions: Dirichlet's theorem and more

These proofs are of comparable difficulty to those we shall encounter in the course. If you find any of these questions to be difficult you should consider whether you wish to proceed with the course.

1. *Modular arithmetic*

   (a) Prove that the equation $x^2 + 4x + 1 = 4y^2$ does not have integer solutions.

   (b) The remainders after division by 20 are $0, 1, 2, 3, \ldots, 19$. We can multiply remainders and then reduce them modulo 20, for example, $7 * 8 = 56 \equiv 16 \mod 20$. We say that a remainder a modulo 20 is *invertible modulo* 20 if there exists a remainder b modulo 20 such that $a \cdot b$ gives remainder 1. For example, remainder 3 is invertible because $3 * 7 = 21 \equiv 1 \mod 20$. Find all invertible remainders modulo 20.

   (c) Prove that the remainder a modulo 20 is invertible if and only if a is coprime to 20 (i.e. that a and 20 do not have common divisors except for 1).

   (d) Find remainders of 7^k modulo 13 for all positive integer k. Can you think of what 7^{-1} mod 13 would be?

2. *Complex numbers*

   (a) Rewrite the following numbers in polar coordinates:

   - $6 + 8i$,
   - $\sqrt{2} - \frac{3}{4}i$,
   - $85 - 85i$,
   - $2.6i$,
   - $-\sqrt{3}$.

(b) A complex root of unity of order k is a complex number z such that $z^k = 1$. Prove that $\frac{1}{2} + \frac{\sqrt{3}}{2}i$ is a root of unity of order 6.

(c) Find all roots of unity of order 4 and 5. You can write them in polar coordinates.

(d) Let us define $e^{i\alpha} = \cos\alpha + i\sin\alpha$. Prove that $|e^{i\alpha}| = 1$. Is $e^{i\alpha}$ always a root of unity?

3. *Elementary proofs*

(a) Let $y_0 > 0$ be some positive real number, and let $y_n = 1 - e^{-y_{n-1}}$ for $n \geq 1$. Prove that $0 < y_n < 1$ for all $n \geq 1$.

(b) This is a case of 'induction gone bad'. Let $x_1 = 0$ and $x_{n+1} = (n+1)x_n$ for all $n \geq 1$. Let Q_n be the statement '$x_n = n!$'. Show that Q_n implies Q_{n+1}, but that there is no integer n for which Q_n is true.

(c) Prove, by induction, that for any real m there exists an x_0 such that $3^x > x^m$ for all $x \geq x_0$.

(d) For what integers n is

$$\frac{1}{n!} > \frac{8^n}{(2n)!}?$$

4. *Integrals*

(a) Find $F(t) = \int e^t \sin t \, dt$ for all real t.

(b) What is the asymptotic behaviour of this function when $t \to \infty$? When $t \to -\infty$?

(c) When is $F(t)$ increasing? When is $F(t)$ decreasing?

(d) For what parameter A, is the function $A\frac{e^t+e^{-t}}{2} + \sin(t)$ bounded?

Solutions

1. (a) Let us assume that there exist integers x and y such that $x^2 + 4x + 1 = 4y^2$. Then the remainder of $x^2 + 4x + 1$ after division by 4 equals the remainder of $4y^2$ after division by 4. This can be written as

$$x^2 + 4x + 1 \equiv 4y^2 \mod 4.$$

For example, since $7 \cdot 6 = 42 = 8 \cdot 5 + 2$, then $7 \cdot 6$ and $8 \cdot 5 + 2$ should give the same remainders after division by 4, i.e. 2. We first note that we can rearrange the equation to

$$(x + 2)^2 - 3 = 4y^2.$$

The right-hand side is divisible by 4, so gives the remainder 0, so we get

$$(x + 2)^2 - 3 \equiv 0 \mod 4,$$

which is

$$(x + 2)^2 \equiv 3 \mod 4.$$

Now let us answer the following question: is it possible that a square of an integer gives remainder 3 after division by 4?

The answer is no! To prove it we can list all the possible remainders that squares can give in the table below.

The table entries come from the following reasoning: if n has remainder 3 after division by 4, then n^2 has remainder $3^2 - 2 \cdot 4 = 1$ after division by 4.

n	n^2
0	0
1	1
2	0
3	1

The first column is all the possible remainders that n can give after division by 4: $0, 1, 2, 3$. The second column shows that n^2 can give only two remainders modulo 4: 0 and 1. In particular, a square number never gives the remainder 3! Hence $(x + 2)^2 \equiv 3 \mod 4$ has no solutions, and thus the initial equation does not have integer solutions.

(b) One way is to write the multiplication table modulo 20. The table below should be read as follows: if a has a remainder 4 after division by 20, and b has a remainder 7 after division by 20, then ab has a remainder $4 \cdot 7 - 20 = 8$ after division by 20.

×	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	$\boxed{1}$	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2	0	2	4	6	8	10	12	14	16	18	0	2	4	6	8	10	12	14	16	18
3	0	3	6	9	12	15	18	$\boxed{1}$	4	7	10	13	16	19	2	5	8	11	14	17
4	0	4	8	12	16	0	4	8	12	16	0	4	8	12	16	0	4	8	12	16
5	0	5	10	15	0	5	10	15	0	5	10	15	0	5	10	15	0	5	10	15
6	0	6	12	18	4	10	16	2	8	14	0	6	12	18	4	10	16	2	8	14
7	0	7	14	$\boxed{1}$	8	15	2	9	16	3	10	17	4	11	18	5	12	19	6	13
8	0	8	16	4	12	0	8	16	4	12	0	8	16	4	12	0	8	16	4	12
9	0	9	18	7	16	5	14	3	12	$\boxed{1}$	10	19	8	17	6	15	4	13	2	11
10	0	10	0	10	0	10	0	10	0	10	0	10	0	10	0	10	0	10	0	10
11	0	11	2	13	4	15	6	17	8	19	10	$\boxed{1}$	12	3	14	5	16	7	18	9
12	0	12	4	16	8	0	12	4	16	8	0	12	4	16	8	0	12	4	16	8
13	0	13	6	19	12	5	18	11	4	17	10	3	16	9	2	15	8	$\boxed{1}$	14	7
14	0	14	8	2	16	10	4	18	12	6	0	14	8	2	16	10	4	18	12	6
15	0	15	10	5	0	15	10	5	0	15	10	5	0	15	10	5	0	15	10	5
16	0	16	12	8	4	0	16	12	8	4	0	16	12	8	4	0	16	12	8	4
17	0	17	14	11	8	5	2	19	16	13	10	7	4	$\boxed{1}$	18	15	12	9	6	3
18	0	18	16	14	12	10	8	6	4	2	0	18	16	14	12	10	8	6	4	2
19	0	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	$\boxed{1}$

The remainder r is invertible modulo 20 if there is the number 1 in the r-line in the table above. For example, the number 13 is invertible modulo 20 because there is a 1 in the intersection of the 13-row and 17-column (which means that $13 \cdot 17$ gives remainder 1 modulo 20). We get that $1, 3, 7, 9, 11, 13, 17$, and 19 are invertible remainders modulo 20.

(c) We can check that numbers $1, 3, 7, 9, 11, 13, 17$, and 19 are the only numbers from 1 to 20, which are coprime to 20.

Another way to prove this fact is to show that a and 20 are coprime if and only if there are two integer numbers m and n such that $am + 20n = 1$. You can check this statement for $1, 3, 7, 9, 11, 13, 17$, and 19.

(d) We create a table of remainders of 7^k after division by 13 below. We see that 7^6 gives the remainder 12 after division by 13, which coincides with the remainder of -1 after division by 13. Why do we write both 12 and -1? Because if 7^6 and -1 have the same remainders modulo 13, it is easy to notice that 7^{12} and $(-1)^2 = 1$ give the same remainders modulo 13. Hence, the remainder of 7^{12} after division by 13 is 1.

k	$7^k \mod 13$
1	7
2	10
3	5
4	9
5	11
6	12 or -1
7	6 or -7
8	3 or -10
9	8 or -5
10	4 or -9
11	2 or -11
12	1
13	7
14	10
...	...

We see that the pattern repeats with the period of length 12. We can also note that 7^6 corresponds to half of the pattern when all remainders are multiplied by -1. Since $7^{12} = 7 \cdot 7^{11} \equiv 1 \mod 7$, we can say that 7^{11} is inverse to 7 modulo 13. If we didn't have to find the powers of 7 modulo 13, we could just note that $2 \cdot 7 = 14 \equiv 1 \mod 13$, and hence, that 2 is inverse to 7 modulo 13. Thus, we get $2 \equiv 7^{-1} \equiv 7^{11} \mod 13$.
Important remark! We can work with $a^{-1} \mod n$ only when $(a, n) = 1$.

2. (a) Converting from rectangular form to polar form involves the formula $z = x + iy = re^{i\theta}$ for $r = |z| = \sqrt{x^2 + y^2}$ and $\tan\theta = y/x$. Note that this implies there are infinitely many possible values for θ — we usually choose the value in $[-\pi, \pi)$.
For $6 + 8i$, we would have $r = 10$ and $\theta = \tan^{-1}(4/3)$. The others follow similarly, except for $2.6i = 2.6e^{\frac{\pi}{2}i}$, which might be best found by looking at $2.6i$ on the complex plane; and $-\sqrt{3}$ is the same in polar form.

   (b) First re-write $\frac{1}{2} + \frac{\sqrt{3}}{2}i = e^{i\theta}$ for $\theta = \tan^{-1}\sqrt{3} = \pi/3$. We then have

$$\left(e^{\frac{\pi}{3}i}\right)^6 = e^{2\pi i} = 1.$$

   (c) A root of unity z of order 5 must satisfy the equation $z^5 = 1$. First note that this means $|z| = r = 1$, so their general form is $z = e^{i\theta}$. Since we can write $1 = e^{2\pi i n}$ for any integer n, the values of θ correspond to those satisfying $z^5 = e^{5i\theta} = e^{2\pi i n}$, which is

$$\theta = \frac{2\pi n}{5} = \ldots, \frac{4\pi}{5}, \frac{2\pi}{5}, 0, \frac{2\pi}{5}, \frac{4\pi}{5}, \frac{6\pi}{5}, \frac{8\pi}{5}, 2\pi, \ldots.$$

The roots of unity of order 5 are thus considered to be those $z = e^{i\theta}$ with the five values of $\theta \in [0, 2\pi)$. We get

$$z = e^{i\theta}, \quad \theta \in \left\{0, \frac{2\pi}{5}, \frac{4\pi}{5}, \frac{6\pi}{5}, \frac{8\pi}{5}\right\}.$$

We can apply a similar argument to the roots of order 4 and get

$$z = e^{i\theta}, \quad \theta \in \left\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\right\}.$$

In this case, it is easy to find the Cartesian form of z, $z = \pm i, \pm 1$.

(d) By the identity $\cos^2 x + \sin^2 x = 1$ we have

$$|\cos\alpha + i\sin\alpha| = \sqrt{\cos^2\alpha + \sin^2\alpha} = 1.$$

Let us show that $e^{i\alpha}$ is a root of unity if and only if $\frac{\alpha}{\pi}$ is rational. Indeed, $e^{i\alpha}$ is a root of unity if and only if there exists an integer q such that

$$(e^{i\alpha})^q = 1,$$

which is equivalent to

$$e^{q\alpha i} = 1,$$

and thus to $q\alpha i = 2\pi i \cdot p$ for some integer p. We can rewrite this equation as follows

$$\frac{\alpha}{\pi} = \frac{2p}{q},$$

for some integer p and q. The last equation is equivalent to $\frac{\alpha}{\pi}$ being rational since any rational number can be represented as $\frac{2p}{q}$ for some integer p and q (the fraction does not have to be irreducible).

3. (a) For all $x > 0$ we know that $0 < 1 - e^{-x} < 1$. Hence, we can prove that $0 < y_n < 1$ if we can prove that $y_n = 1 - e^{-y_{n-1}}$ implies $y_n > 0$ for all $n \geq 0$. This will be the case if $e^{-y_{n-1}} < 1$, equivalently $y_{n-1} > 0$, for all $n \geq 1$. Fortunately, we are told it is true for y_0. Beyond this, it is equivalent to the condition $y_n > 0$ for all $n \geq 1$.

(b) If $x_n = n!$ then $x_{n+1} = (n+1)x_n = (n+1)n! = (n+1)!$, which proves that $Q_n \Rightarrow Q_{n+1}$. However, to have $x_n = n!$ we would need $x_n \neq 0$ for all $n \geq 1$, as if this was the case, it would imply $x_n = 0$ for all $n \geq 1$, and it is not possible to have $n! = 0$ for any $n \geq 1$. Thus, the fact that $x_1 = 0$ implies that there is no $n \geq 1$ for which Q_n is true.

(c) The statement $3^x > x^m$ implies

$$\frac{x}{\log x} > \frac{m}{\log 3}.$$

As m is a fixed number, and the LHS is an increasing function, we know that this statement will be true for sufficiently large x. To determine the values of x for which the LHS is increasing, we can solve for when the derivative is positive. We find that

$$\begin{aligned}\frac{d}{dx}\left(\frac{x}{\log x}\right) = \frac{1}{\log x} - \frac{1}{\log^2 x} &> 0 \\ \Rightarrow \log x &> 1.\end{aligned}$$

Hence, the function $x/\log x$ is increasing for all $x > e$. Therefore, there must exist some $x_0 > e$ for which the original statement is true for all $x \geq x_0$.

(d) This inequality is equivalent to

$$\prod_{i=n+1}^{2n} i > 8^n.$$

The left-hand side is a product of n values, starting at $n+1$. As such, it is bounded below by $(n+1)^n$. This implies that the original inequality will be true if $(n+1)^n > 8^n$. This is indeed the case for any $n \geq 8$, as we would have $n+1 > 8$. For values below this, it is possible to check numerically, and we find that the largest exception is at $n = 5$. Hence, the original statement is true for all $n \geq 6$.

4. (a) Using integration by parts twice gives

$$\begin{aligned}F(t) &= e^t \sin(t) - \int e^t \cos(t) dt \\ &= e^t \sin(t) - \left(e^t \cos(t) + \int e^t \sin(t) dt\right) + c \\ &= e^t \sin(t) - e^t \cos(t) - F(t) + c,\end{aligned}$$

where c is some constant appearing because of integration. Rearranging, this implies

$$F(t) = \frac{e^t}{2}\left(\sin(t) - \cos(t)\right) + c,$$

where now c denotes a different constant.

(b) We will prove that as $t \to \infty$, the function F takes arbitrarily large positive and negative values.

Let us look at the function $\sin(t) - \cos(t)$. There are infinitely many points $t_k \to \infty$ of the form $t_k = \pi k + \frac{\pi}{2}$, k a positive integer, such that $\sin(t_k) - \cos(t_k) = 1$. There are also infinitely many points $s_k \to \infty$ of the form $s_k = \pi k$, k a positive integer, such that $\sin(s_k) - \cos(s_k) = -1$. Hence, $F(t_k) = \frac{e^t}{2} + c$ can be arbitrarily large positive number, and $F(s_k) = -\frac{e^t}{2} + c$ can be an arbitrarily large negative number.

Hence, as $t \to \infty$, $F(t)$ will be unbounded, and fluctuate between increasingly larger positive and negative values. As $t \to -\infty$ however, e^t approaches zero and $\frac{1}{2}(\sin(t) - \cos(t))$ is bounded between $\sqrt{2}$ and $\sqrt{2}$, and hence $F(t)$ approaches c.

(c) The function $\sin(t)$ is bounded between -1 and -1 for all t. The function $\frac{e^t+e^{-t}}{2}$ tends to infinity as $t \to \infty$ because

$$\frac{e^t + e^{-t}}{2} \geq \frac{e^t}{2}$$

for all t. Hence if $A \neq 0$, then $A\frac{e^t+e^{-t}}{2}$ tends to $\pm\infty$ as $t \to \infty$ depending on the sign of A. If $A = 0$, then the initial function is equal to $\sin(t)$ and, thus, is bounded.