

Answer **all** the questions.

Question 1 [30 marks]

- (a) State, without proof, two equivalent statements of the fifth axiom in Euclidean geometry on the plane.
- (b) Gauss wrote in a private letter, asserting that “*The assumption that (in a triangle) the sum of the three angles is less than 180° leads to a curious geometry, quite different from ours, but thoroughly consistent, which I have developed to my entire satisfaction.*” Explain in detail the content of the above statement, together with important historical developments leading to the discovery of Non-Euclidean geometry.
- (c) In the following (i) and (ii), we assume the first four axioms in Euclidean geometry on the plane, and that the exterior angle θ of any triangle is bigger than or equal to the sum of the opposite angles $\theta_1 + \theta_2$ (see the figure). But we do *not* take the fifth axiom for granted.

- (i) In the figure below, explain why $\phi \rightarrow 0$ as $|OP| \rightarrow \infty$. Here $|OP|$ is the distance between the points O and P . The point O is fixed, whereas the point P ‘slides’ along the given line toward infinity. (Consider using isosceles triangles.)

- (ii) Assume also the non-Euclidean axiom:

(N) *Given a line ℓ_1 and a point P not on the line, there are at least two lines ℓ_2 and ℓ_3 that pass through P and are parallel to ℓ_1 .*

Explain how to use the result in (i) above to construct a triangle with the sum of the three interior angles *less* than 180° .

Question 2 [20 marks]

A geodesic triangle on the unit sphere is bounded by three arcs of great circles such that no two arcs are in the same great circle, and any two arcs meet at exactly one point.

- (i) On the unit sphere, describe how to construct a geodesic triangle whose interior angles summed up to be *more* than 360° .
- (ii) State the Archimedes theorem for the map from the unit sphere to the cylinder circumscribing the sphere. Explain how to use the Archimedes theorem to prove Girard's theorem, which says that the sum of the three interior angles of a geodesic triangle on the unit sphere is equal to the area of the triangle plus π .
- (iii) It is conjectured that the sum of the three interior angles of *any* geodesic triangle on the unit sphere cannot be more than 3π . Do you think that this is correct? Provide a counter-example if you think the conjecture is wrong, or else a proof if correct. Recall that the area of the unit sphere is 4π .

Question 3 [15 marks]

"I found working with Carl (Cornell's postdoctoral supervisor) to be a very congenial experience. Carl and I share very similar tastes in what makes for an interesting physics experiment, and I was happy to assimilate a fraction of his seemingly endless bag of technological ideas. Carl taught me to decide what part of the experimental apparatus really mattered, and then to spare no effort improving that part. Conversely, Carl emphasized that one needs to recognize where 'good enough' was indeed good enough, and to waste no time worrying about it." – E. Cornell (Nobel Laureates in Physics, 2001).

"I spent most of my intellectual and psychic energy ... on a (mathematics course) taught by Raoul Bott at Harvard. Bott not only taught the details of (the proofs), but also, much more deeply, how mathematicians truly think. He taught how to divide the meat of a proof from the detail. In this course I learned to respect the variety of mathematical structure that can be used to describe a problem." – G. Akerlof (Nobel Laureates in Economic Sciences, 2001).

Drawing insight from the above paragraphs, discuss in detail the notion of "apprentice" in scientific and mathematical thinking. Provide another example in mathematics to illuminate your discussion.

Question 4 [35 marks]

Here we use the slightly restricted notion of module

$$a \equiv r \pmod{n}$$

to denote “when a is divided by n , the remainder is r ”, where a and n are positive integers, and $0 \leq r < n$ is an integer.

(i) Show that if

$$a \equiv r \pmod{n},$$

then the remainder of a^k when it is divided by n is equal to the remainder of r^k when it is divided by n . Here k is a positive integer. (*Hint*: Consider using the mathematical induction.)

(ii) The Fermat little theorem says that if $p > 1$ is a prime number and $0 < a < p$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

(You are NOT required to prove the Fermat little theorem.) Using the Fermat little theorem, or otherwise, show that if b is a positive integer which cannot be divided by p , then

$$b^{p-1} \equiv 1 \pmod{p}. \quad (3.1)$$

(*Hint*: Consider the remainder R in $b \equiv R \pmod{p}$.)

(iii) As a consequence of the Lagrange theorem, we know that if $n = p \times q$ is a pseudo-prime, where p and q are *distinct* prime numbers bigger than 1, and c is an integer with $0 < c < n$, then

$$c^{(p-1)(q-1)+1} \equiv c \pmod{n}. \quad (3.2)$$

Consider

$$c^{(p-1)(q-1)} \equiv \bar{R} \pmod{n}. \quad (3.3)$$

Show that in the case when $c = 3$, $p = 3$ and $q = 5$, the remainder \bar{R} in (3.3) does not equal to 1.

It is conjectured that \bar{R} in (3.3) is always equal to 1 if p does not divide c and q does not divide c . Do you think that this is correct? Provide a counter-example if you think the conjecture is wrong, or else a proof if correct.

–Question 4 continues on the next page.–

- (iv) Given that $p \neq q$ are prime numbers bigger than one, we seek to establish a generalized version of (3.2). First, explain why p and q cannot both divide c . (Recall that $c < n$.) Without loss of generality, we may assume that p does not divide c . Using the result in (i) and (ii) *only* [in particular, we do not use (3.2) and (3.3)], prove that

$$c^{k(p-1)(q-1)} \equiv 1 \pmod{p}. \quad (3.4)$$

Here k is a positive integer. [*Hint:* $c^{k(p-1)(q-1)} = (c^{p-1})^{k(q-1)}$, apply (3.1) to c^{p-1} .] Show that (3.4) leads to

$$c^{k(p-1)(q-1)+1} \equiv c \pmod{p}.$$

That is, p can divide $c^{k(p-1)(q-1)+1} - c$. Similarly, explain why q can divide $c^{k(p-1)(q-1)+1} - c$. (Beware of the possibility that q can divide c .) Finally, show that

$$c^{k(p-1)(q-1)+1} \equiv c \pmod{n} (= p \times q).$$

–End of The Paper.–