Basic Algebra

2. Rings — Continued – Prime rings

Marin Mersenne† **(1588-1648)**

Pierre de Fermat†† **(1601-1665)**

In the following A_m denotes a prime ring of characteristic m, for example $\mathrm{A}_m = \mathbb{Z}/\mathbb{Z}m$.

2.1. Let A be a commutative ring. The ring of numerical functions with values in A (cf. Exercsie 1.2) is an integral domain if and only if A is an integral domain.

2.2. Let A be a finite commutative ring and let a be the product of all non-zero elements of A. Then :

$$a = \begin{cases} -1, & \text{if } A \text{ is a field}; \\ 2, & \text{if } A \text{ is a prime ring with 4 elements}; \\ 0, & \text{otherwise}. \end{cases}$$

(**Hint:** Use the exercises T2.1 a) and T2.2 .)

2.3. Let Q be the quotient field of the integral domain A. Then $\mathrm{card}(Q) = \mathrm{card}(A)$.

(**Hint :** For an infinite set X, $\mathrm{card}(X \times X) = \mathrm{card}(X)$ –this can be easily proved by using Zorn's lemma.)

2.4. A Fermat-number $2^{2^t} + 1$ with $t \in \mathbb{N}$ can have only prime divisors of the form $n2^{t+1} + 1$ with $n \in \mathbb{N}^*$. (**Hint :** Use a method of proof as in T2.4.)

2.5. Let $m \in \mathbb{N}^*$, and $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the (normalised) prime factorisation of m.

a). For $s \in \mathbb{Z}$ the following statements are equivalent:

(1) $s \cdot 1_{\mathrm{A}_m}$ is nilpotent in A_m. (2) s is a multiple of $p_1 \cdots p_r$.

b). A_m has exactly 2^r idempotent elements. (The natural numbers e with $0 \leq e < m$ and $e \equiv e^2 \bmod m$ can be calculated (by using T2.6) in the direct product of prime rings of characteristic p^{α_i}, $i = 1, \ldots, r$ and hence one can reduce the problem to the case $r = 1$.)

2.6. Let p be a prime number ≥ 3.

a). In the unit group $\mathrm{A}_p^\times$, the element -1 is the only element of order 2.

b). (Wilson's Theorem). $(p-1)! \equiv -1 \bmod p$. (**Hint :** Apply 2.2 to the prime ring A_p.)

c). (Euler's criterion for the quadartic residues) Let $a \in \mathbb{Z}$ be not divisible by p. If there exists $b \in \mathbb{Z}$ with $b^2 \equiv a \bmod p$, then $a^{(p-1)/2} \equiv 1 \bmod p$. Further, if there is no $b \in \mathbb{Z}$ with $b^2 \equiv a \bmod p$, then $a^{(p-1)/2} \equiv -1 \bmod p$.(**Hint :** Apply T2.1 b) to the group $\mathrm{A}_p^\times$.)

d). If $p \equiv 1 \bmod 4$, then $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \bmod p$ and if $p \equiv 3 \bmod 4$, then there exists no $b \in \mathbb{Z}$ with $b^2 \equiv -1 \bmod p$.

e). (Converse of the Wilson's theorem) If $n \in \mathbb{N}$, $n > 1$, and if $(n-1)! \equiv -1 \bmod n$, then n is a prime number. (**Hint :** Apply 2.2 b) to the ring A_p. **Second Proof** (Pranesachar)**:** Note that either if n has two distinct prime factors p and q or if n has a square factor p^2 with p odd prime, then n divides $(n-1)!$. In the remaining case $n = 2^2 = 4$ and $(n-1)! \bmod n = 3! \equiv \bmod 4 \equiv 2 \bmod 4 \not\equiv 1 \bmod 4$.)

On the backside one can see (simple) test-exercises.

Test-Exercises

T2.1. Let G be a finite abelian group with identity element e and with only one element f of order 2. Then Ord $G = 2n$ with $n \in \mathbb{N}^*$. Further,

a). $\prod_{x\in G} x = f$.

b). Let $a \in G$. If there exists a $b \in G$ with $b^2 = a$, then $a^n = e$, in the other case $a^n = f$. (**Hint :** If a is not a square in G, then the relation: $c \sim d$ if and only if $c = d$ or $cd = a$ is an equivalence relation in G, all the equivalence classes contain exactly two elements. Let $K(1), \ldots, K(n)$ be these equivalence classes. Then $a^n = \prod_{i=1}^{n}(\prod_{y\in K(i)} y) = \prod_{x\in G} x = f$.)

T2.2. In a finite ring every non-zero divisor is a unit. In particular, a non-zero domain is a divison ring. (**Remark :** A famous theorem of Wedderburn states that : *every finite division ring is commutative and hence a field*.)

T2.3. Let a and b be non-zero relatively prime integers. Then the sum $a^{\varphi(|b|)} + b^{\varphi(|a|)} \equiv 1 \mod ab$.

T2.4. a). A Mersenne number $2^p - 1$ with p prime and $p > 2$ can have only prime divisors of the form $2np + 1$ with $n \in \mathbb{N}^*$. (**Hint :** If q is a prime divisor of $2^p - 1$, p prime, then the order of $2 \cdot 1_{\mathrm{A}_q}$ in the unit group of A_q is equal to p.)

b). Every two distinct Mersenne numbers are relatively prime.

T2.5. Let A be a ring of characteristic $m > 0$. For an integer r, the following statements are equivalent: (1) $r \cdot 1_A$ is a unit in A. (2) $r \cdot 1_A$ is a unit in the prime ring of A. (3) $\gcd(r, m) = 1$.

T2.6. Let $m_1, \ldots, m_r$ be non-zero pairwise relatively prime natural numbers and $m := m_1 \cdots m_r$. Then $A := \prod_{i=1}^{r} \mathrm{A}_{m_i}$ is a prime ring of the characteristic m. the unit group of A is the direct product of the unit groups of the prime rings A_{m_i}. What can you now conclude for the Euler's φ-function?

---

† **Marin Mersenne (1588-1648)** Marin Mersenne was born on 8 Sept 1588 in Oize in Maine, France and died on 1 Sept 1648 in Paris, France Marin Mersenne attended school at the College of Mans, then, from 1604 spent five years in the Jesuit College at La Fleche. From 1609 to 1611 he studied theology at the Sorbonne. Mersenne joined the religious order of the Minims in 1611. The name of the order comes since the Minims regard themselves as the least (minimi) of all the religious; they devote themselves to prayer, study and scholarship. Mersenne continued his education within the order at Nigeon and then at Meaux. He returned to Paris where in 1612 he became a priest at the Place Royale.

He taught philosophy at the Minim convent at Nevers from 1614 to 1618. In 1619 he returned again to Paris to the Minims de l'Annociade near Place Royale. His cell in Paris became a meeting place for Fermat, Pascal, Gassendi, Roberval, Beaugrand and others who later became the core of the French Academy. Mersenne corresponded with other eminent mathematicians and he played a major role in communicating mathematical knowledge throughout Europe at a time when there were no scientific journals.

Mersenne investigated prime numbers and he tried to find a formula that would represent all primes. Although he failed in this, his work on numbers of the form 2^p-1 , p prime has been of continuing interest in the investigation of large primes. It is easy to prove that if the number $n=2^p-1$ is prime then p must be a prime. In 1644 Mersenne claimed that n is prime if p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 and 257 but composite for the other 44 primes smaller than 257.

Over the years it has been found that Mersenne was wrong about 5 of the primes less than or equal to 257 (he claimed two that did not lead to a prime (67 and 257) and missed 3 that did: 61, 89, 107).

Mersenne defended Descartes and Galileo against theological criticism and struggled to expose the pseudo sciences of alchemy and astrology. He continued some of Galileo's work in acoustics and stimulated some of Galileo's own later discoveries. He proposed the use of the pendulum as a timing device to Huygens, thus inspiring the first pendulum clock. In 1633 Mersenne published Traité des mouvements, and in 1634 he published Les Méchanique de Galilée which was a version of Galileo's lectures on mechanics. He translated parts of Galileo's Dialogo into French and in 1639 he published a transation of Galileo's Discorsi. It is through Mersenne that Galileo's work became known outside Italy.

Two important publications in mathematical physics were L'Harmonie Universelle (1636) and Cogitata Physico-Mathematica (1644). Mersenne also wrote Traité d'harmonie universelle (1627), a work on music, musical instruments and acoustics. After his death letters in his cell were found from 78 different correspondents including Fermat, Huygens, Pell, Galileo and Torricelli.

---

† **Pierre De Fermat (1601-1665)** was born on 17 Aug 1601 in Beaumont-de-Lomagne, France and died on 12 Jan 1665 in Castres, France. Pierre Fermat's father was a wealthy leather merchant and second consul of Beaumont- de- Lomagne. Pierre had a brother and two sisters and was almost certainly brought up in the town of his birth. Although there is little evidence concerning his school education it must have been at the local Franciscan monastery.

He attended the University of Toulouse before moving to Bordeaux in the second half of the 1620s. In Bordeaux he began his first serious mathematical researches and in 1629 he gave a copy of his restoration of Apollonius's Plane loci to one of the mathematicians there. Certainly in Bordeaux he was in contact with Beaugrand and during this time he produced important work on maxima and minima which he gave to Etienne d'Espagnet who clearly shared mathematical interests with Fermat.

From Bordeaux Fermat went to Orléans where he studied law at the University. He received a degree in civil law and he purchased the offices of councillor at the parliament in Toulouse. So by 1631 Fermat was a lawyer and government official in Toulouse and because of the office he now held he became entitled to change his name from Pierre Fermat to Pierre de Fermat.

For the remainder of his life he lived in Toulouse but as well as working there he also worked in his home town of Beaumont-de-Lomagne and a nearby town of Castres. From his appointment on 14 May 1631 Fermat worked in the lower chamber of the parliament but on 16 January 1638 he was appointed to a higher chamber, then in 1652 he was promoted to the highest level at the criminal court. Still further promotions seem to indicate a fairly meteoric rise through the profession but promotion was done mostly on seniority and the plague struck the region in the early 1650s meaning that many of the older men died. Fermat himself was struck down by the plague and in 1653 his death was wrongly reported, then corrected:

I informed you earlier of the death of Fermat. He is alive, and we no longer fear for his health, even though we had counted him among the dead a short time ago.

The following report, made to Colbert the leading figure in France at the time, has a ring of truth:

Fermat, a man of great erudition, has contact with men of learning everywhere. But he is rather preoccupied, he does not report cases well and is confused.

Of course Fermat was preoccupied with mathematics. He kept his mathematical friendship with Beaugrand after he moved to Toulouse but there he gained a new mathematical friend in Carcavi. Fermat met Carcavi in a professional capacity since both were councillors in Toulouse but they both shared a love of mathematics and Fermat told Carcavi about his mathematical discoveries.

In 1636 Carcavi went to Paris as royal librarian and made contact with Mersenne and his group. Mersenne's interest was aroused by Carcavi's descriptions of Fermat's discoveries on falling bodies, and he wrote to Fermat. Fermat replied on 26 April 1636 and, in addition to telling Mersenne about errors which he believed that Galileo had made in his description of free fall, he also told Mersenne about his work on spirals and his restoration of Apollonius's Plane loci. His work on spirals had been motivated by considering the path of free falling bodies and he had used methods generalised from Archimedes' work On spirals to compute areas under the spirals. In addition Fermat wrote:

I have also found many sorts of analyses for diverse problems, numerical as well as geometrical, for the solution of which Viète's analysis could not have sufficed. I will share all of this with you whenever you wish and do so without any ambition, from which I am more exempt and more distant than any man in the world.

It is somewhat ironical that this initial contact with Fermat and the scientific community came through his study of free fall since Fermat had little interest in physical applications of mathematics. Even with his results on free fall he was much more interested in proving geometrical theorems than in their relation to the real world. This first letter did however contain two problems on maxima which Fermat asked Mersenne to pass on to the Paris mathematicians and this was to be the typical style of Fermat's letters, he would challenge others to find results which he had already obtained.

Roberval and Mersenne found that Fermat's problems in this first, and subsequent, letters were extremely difficult and usually not soluble using current techniques. They asked him to divulge his methods and Fermat sent Method for determining Maxima and Minima and Tangents to Curved Lines, his restored text of Apollonius's Plane loci and his algebraic approach to geometry Introduction to Plane and Solid Loci to the Paris mathematicians.

His reputation as one of the leading mathematicians in the world came quickly but attempts to get his work published failed mainly because Fermat never really wanted to put his work into a polished form. However some of his methods were published, for example Hérigone added a supplement containing Fermat's methods of maxima and minima to his major work Cursus mathematicus. The widening correspondence between Fermat and other mathematicians did not find universal praise. Frenicle de Bessy became annoyed at Fermat's problems which to him were impossible. He wrote angrily to Fermat but although Fermat gave more details in his reply, Frenicle de Bessy felt that Fermat was almost teasing him.

However Fermat soon became engaged in a controversy with a more major mathematician than Frenicle de Bessy. Having been sent a copy of Descartes' La Dioptrique by Beaugrand, Fermat paid it little attention since he was in the middle of a correspondence with Roberval and Etienne Pascal over methods of integration and using them to find centres of gravity. Mersenne asked him to give an opinion on La Dioptrique which Fermat did describing it as *groping about in the shadows.*

He claimed that Descartes had not correctly deduced his law of refraction since it was inherent in his assumptions. To say that Descartes was not pleased is an understatement. Descartes soon found reason to feel even more angry since he viewed Fermat's work on maxima, minima and tangents as reducing the importance of his own work La Géométrie which Descartes was most proud of and which he sought to show that his Discours de la méthod alone could give.

Descartes attacked Fermat's method of maxima, minima and tangents. Roberval and Etienne Pascal became involved in the argument and eventually so did Desargues who Descartes asked to act as a referee. Fermat proved correct and eventually Descartes admitted this writing:

... seeing the last method that you use for finding tangents to curved lines, I can reply to it in no other way than to say that it is very good and that, if you had explained it in this manner at the outset, I would have not contradicted it at all.

Did this end the matter and increase Fermat's standing? Not at all since Descartes tried to damage Fermat's reputation. For example, although he wrote to Fermat praising his work on determining the tangent to a cycloid (which is indeed correct), Descartes wrote to Mersenne claiming that it was incorrect and saying that Fermat was inadequate as a mathematician and a thinker. Descartes was important and respected and thus was able to severely damage Fermat's reputation.

The period from 1643 to 1654 was one when Fermat was out of touch with his scientific colleagues in Paris. There are a number of reasons for this. Firstly pressure of work kept him from devoting so much time to mathematics. Secondly the Fronde, a civil war in France, took place and from 1648 Toulouse was greatly affected. Finally there was the plague of 1651 which must have had great consequences both on life in Toulouse and of course its near fatal consequences on Fermat himself. However it was during this time that Fermat worked on **number theory**.

Fermat is best remembered for this work in number theory, in particular for **Fermat's Last Theorem**. This theorem states that $x^n+y^n=z^n$ has no non-zero integer solutions for x, y and z when n > 2. Fermat wrote, in the margin of Bachet's translation of Diophantus's Arithmetica *I have discovered a truly remarkable proof which this margin is too small to contain.*

These marginal notes only became known after Fermat's son Samuel published an edition of Bachet's translation of Diophantus's Arithmetica with his father's notes in 1670.

It is now believed that Fermat's 'proof' was wrong although it is impossible to be completely certain. The truth of Fermat's assertion was proved in June 1993 by the British mathematician Andrew Wiles, but Wiles withdrew the claim to have a proof when problems emerged later in 1993. In November 1994 Wiles again claimed to have a correct proof which has now been accepted. Unsuccessful attempts to prove the theorem over a 300 year period led to the discovery of commutative ring theory and a wealth of other mathematical discoveries.

Fermat's correspondence with the Paris mathematicians restarted in 1654 when Blaise Pascal, Etienne Pascal's son, wrote to him to ask for confirmation about his ideas on probability. Blaise Pascal knew of Fermat through his father, who had died three years before, and was well aware of Fermat's outstanding mathematical abilities. Their short correspondence set up the theory of probability and from this they are now regarded as joint founders of the subject. Fermat however, feeling his isolation and still wanting to adopt his old style of challenging mathematicians, tried to change the topic from probability to number theory. Pascal was not interested but Fermat, not realising this, wrote to Carcavi saying:

I am delighted to have had opinions conforming to those of M Pascal, for I have infinite esteem for his genius... the two of you may undertake that publication, of which I consent to your being the masters, you may clarify or supplement whatever seems too concise and relieve me of a burden that my duties prevent me from taking on.

However Pascal was certainly not going to edit Fermat's work and after this flash of desire to have his work published Fermat again gave up the idea. He went further than ever with his challenge problems however:

Two mathematical problems posed as insoluble to French, English, Dutch and all mathematicians of Europe by Monsieur de Fermat, Councillor of the King in the Parliament of Toulouse.

His problems did not prompt too much interest as most mathematicians seemed to think that number theory was not an important topic. The second of the two problems, namely to find all solutions of $Nx^2+1=y^2$ for N not a square, was however solved by Wallis and Brouncker and they developed **continued fractions** in their solution. Brouncker produced rational solutions which led to arguments. Frenicle de Bessy was perhaps the only mathematician at that time who was really interested in number theory but he did not have sufficient mathematical talents to allow him to make a significant contribution.

Fermat posed further problems, namely that the sum of two cubes cannot be a cube (a special case of Fermat's Last Theorem which may indicate that by this time Fermat realised that his proof of the general result was incorrect), that there are exactly two integer solutions of $x^2+4=y^3$ and that the equation $x^2+2=y^3$ has only one integer solution. He posed problems directly to the English. Everyone failed to see that Fermat had been hoping his specific problems would lead them to discover, as he had done, deeper theoretical results.

Around this time one of Descartes' students was collecting his correspondence for publication and he turned to Fermat for help with the Fermat - Descartes correspondence. This led Fermat to look again at the arguments he had used 20 years before and he looked again at his objections to Descartes' optics. In particular he had been unhappy with Descartes' description of refraction of light and he now settled on a principle which did in fact yield the sine law of refraction that Snell and Descartes had proposed. However Fermat had now deduced it from a fundamental property that he proposed, namely that light always follows the shortest possible path. Fermat's principle, now one of the most basic properties of optics, did not find favour with mathematicians at the time.

In 1656 Fermat had started a correspondence with Huygens. This grew out of Huygens interest in probability and the correspondence was soon manipulated by Fermat onto topics of number theory. This topic did not interest Huygens but Fermat tried hard and in New Account of Discoveries in the Science of Numbers sent to Huygens via Carcavi in 1659, he revealed more of his methods than he had done to others.

Fermat described his method of infinite descent and gave an example on how it could be used to prove that every prime of the form 4k + 1 could be written as the sum of two squares. For suppose some number of the form 4k + 1 could not be written as the sum of two squares. Then there is a smaller number of the form 4k + 1 which cannot be written as the sum of two squares. Continuing the argument will lead to a contradiction. What Fermat failed to explain in this letter is how the smaller number is constructed from the larger. One assumes that Fermat did know how to make this step but again his failure to disclose the method made mathematicians lose interest. It was not until Euler took up these problems that the missing steps were filled in.

Fermat is described as

Secretive and taciturn, he did not like to talk about himself and was loath to reveal too much about his thinking. ... His thought, however original or novel, operated within a range of possibilities limited by that [1600 - 1650] time and that [France] place.

Carl B Boyer in his writing, says:

Recognition of the significance of Fermat's work in analysis was tardy, in part because he adhered to the system of mathematical symbols devised by François Viète, notations that Descartes' Géométrie had rendered largely obsolete. The handicap imposed by the awkward notations operated less severely in Fermat's favourite field of study, the theory of numbers, but here, unfortunately, he found no correspondent to share his enthusiasm.