E0 221 Discrete Structures / August-December 2013

(ME, MSc, Ph. D. Programmes)

Download from : http://www.math.iisc.ernet.in/patil/courses/courses/Current Courses/...

Tel : +91-(0)80-2293 2239/(Maths Dept. 3212) **E-mails :** dppatil@csa.iisc.ernet.in / patil@math.iisc.ernet.in

Lectures : Monday and Wednesday ; 10:00–11:30 **Venue:** CSA, Lecture Hall (Room No. 117)

TAs/Corrections by : **Akanksha Agrawal** (akanksha.agrawal@csa.iisc.ernet.in)
Palash Dey (palash@csa.iisc.ernet.in) / **Govind Sharma** (govindjsk@csa.iisc.ernet.in)
Sayantan Mukheriee (sayantan.mukherjee@csa.iisc.ernet.in)

Quizzes : During Wednesday, Lectures on **Aug 28; Sept 18; (Monday) Oct 14; Oct 30;** **Time :** 10:00 -10:15

1-st Midterm : Sunday, September 15, 2013; 14:00 -16:30 **2-nd Midterm :** Saturday, October 12, 2013; 10:00 -12:00

Final Examination : Saturday, December 07, 2013, 14:00 -17:00

Evaluation Weightage : Quizzes (Four) + Midterms (Two) : 50% **Final Examination :** 50%

Range of Marks for Grades (Total 100 Marks)						
	Grade S	**Grade A**	**Grade B**	**Grade C**	**Grade D**	**Grade F**
Marks-Range	> 90	76–90	61–75	46–60	35–45	< 35

5. The Natural Numbers

- **Solution of the Exercise *5.10 carries 10 Bonus Points.**
- **Recommended to solve the Exercise ^{R}5.11.**

5.1 (Fibonacci[1] Sequence) The sequence f_n, $n \in \mathbb{N}$, defined recursively by $f_0 = 0$, $f_1 = 1$ and $f_{n+1} = f_n + f_{n-1}$ for all $n \geq 1$, is called the Fibonacci Sequence[2] and its n-th term f_n is called the n-th Fibonacci number. The first few terms of the Fibonacci Sequence are $0, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$. (**Remark :** The Recursion Theorem T5.7-(a) cannot directly justify its existence, for the value f_{n+1} for $n \geq 1$ depend not only on f_n, but upon f_{n-1} as well. However, we can justify the simultaneous existence of the two sequences f_n and g_n satisfying :

$$\begin{cases} f_0 = 0, & f_{n+1} = f_n + g_n, \quad \text{for} \quad n \geq 0, \\ g_0 = 1, & g_{n+1} = f_n, \quad \text{for} \quad n \geq 0. \end{cases}$$

For this we can use the Simultaneous Recursion (see T5.10-(b)) by taking $(a, b) = (0, 1)$, $H : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is the addition on $\mathbb{N}$ and $K : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is the first projection.)

(a) For the n-th Fibonacci number f_n, prove the following explicit (Binet's Formula[3]) :

$$f_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

(**Remark:** If we put $\Phi := (1+\sqrt{5})/2$, then $\Phi = 1 + \Phi^{-1} = \Phi^2 - 1$, $-\Phi^{-1} = (1-\sqrt{5})/2$ and $f_n = (\Phi^n - (-1)^n \Phi^{-n})/\sqrt{5}$. The number Φ is also denoted by τ. — If $\alpha := \pi/5$, then from the equation $(4\cos^2\alpha - 1 - 2\cos\alpha)\sin\alpha = \sin 3\alpha - \sin 2\alpha = 0$, the equations $4\cos^2\alpha - 2\cos\alpha - 1 = 0$ and $2\cos\alpha = 2\cos(\pi/5) = \Phi$ follow. Consequently, the regular 10-gon (as well as regular pentagon) can be constructed by using the golden-ration.)

(b) Prove the following equalities by induction :

---

[1] Leonard of Pisa or Fibonacci (1170-1250) an Italian Salesman who wrote a book on "Liber Abaci" in 1209 and introduced the Hindu-Arabic place-valued decimal system and the use of Arabic numerals into Europe. Fibonacci played an important role in reviving ancient mathematics and made significant contributions of his own.

[2] In 1844 Gabriel Lamé observed that if n division steps are required in the Euclidean algorithm to compute $\gcd(a, b)$, $a, b \in \mathbb{N}^*$, then $a \geq f_{n+2}$ and $b \geq f_{n+1}$. Therefore the sequence was called the *Lamé sequence*. But Lucas discovered that Fibonacci had been aware of these numbers six centuries earlier.

[3] Binet Jacques Philippe (1786-1856) was a French mathematician who discovered this formula (in 1843) expressing f_n in terms of the integer n. The Binet's formula was already known to Abraham de Moivre (1667-1754) in 1730. Abraham de Moivre was a French mathematician famous for *de Moivre's formula*, which links complex numbers and trigonometry, and for his work on the normal distribution and probability theory. He was a friend of Isaac Newton, Edmund Halley, and James Stirling. De Moivre first discovered Binet's formula, the closed-form expression for Fibonacci numbers linking the n-th power of Φ to the n-th Fibonacci number.

(i) $f_{n+m} = f_{n-1}f_m + f_n f_{m+1}$ for all $m \geq 0$ and all $n \geq 1$.

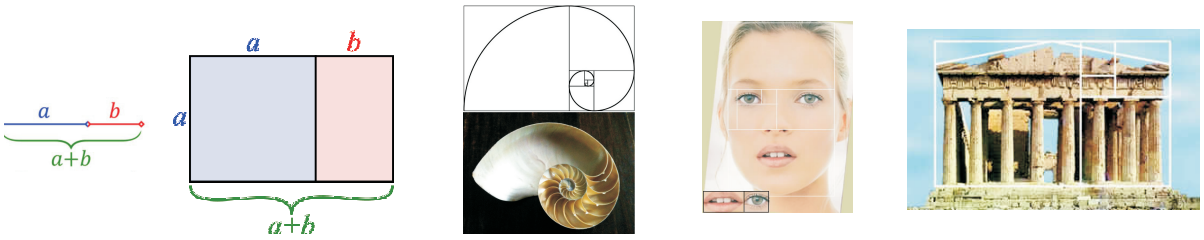
In particular, $f_{2n} = f_n(f_{n-1} + f_{n+1}) = f_{n+1}^2 - f_{n-1}^2$ for all $n \geq 1$.

(ii) $f_n^2 = f_{n-1}f_{n+1} + (-1)^{n+1}$ for all $n \geq 1$.

(iii) $\Phi^n = f_{n-1} + f_n\Phi$, for all $n \in \mathbb{N}^*$. (**Remark :** Using this equality we can define the Fibonacci-numbers f_n for all $n \in \mathbb{Z}$. We then have $f_n = f_{n-1} + f_{n-2}$ for all $n \in \mathbb{Z}$. Then we have $f_n = f_{n-1} + f_{n-2}$ and $f_n = (-1)^{n+1}f_{-n}$ for all $n \in \mathbb{Z}$.)

(c) $f_n = (a^n - b^n)/\sqrt{5}$, where a and b are the positive and negative zeros of the quadratic equation $X^2 - X - 1 = 0$. (**Hint :** Use Binet's Formula.)

(d) Show that the sequence f_{n+1}/f_n, $n \geq 1$, of the successive quotients of Fibonacci-numbers converges to the g o l d e n s e c t i o n $\Phi := \frac{1+\sqrt{5}}{2}$. (Moreover, f_{n+1}/f_n is the $(n-1)$-th approximation-fraction in the continued fraction expansion of $\Phi = [1,1,1,\ldots]$. — In mathematics and the arts, two quantities are in the g o l d e n r a t i o if their ratio is the same as the ratio of their sum to their maximum. The following figure illustrates the geometric relationship:



Algebraically, for a and b with $a > b$, $\frac{a+b}{a} = \frac{a}{b} =: \Phi$, where the Greek letter phi (Φ) represents the golden ratio. Its value is: $\Phi = \frac{1+\sqrt{5}}{2} = 1.61803\,39887\ldots$. The golden ratio is also called the g o l d e n s e c t i o n (in Latin: *sectio aurea*) or g o l d e n m e a n. Many artists and architects have proportioned their works to approximate the golden ratio-especially in the form of the golden rectangle, in which the ratio of the longer side to the shorter is the golden ratio-believing this proportion to be aesthetically pleasing. The golden ratio has also been used to analyze the proportions of natural objects as well as man-made systems. For example, *Flower petals*[4]; *Shells*[5]; *DNA Molecules*; *Faces*[6] (both human and nonhuman); many buildings and artworks such as the *Parthenon in Greece*, but it is not really known if it was designed that way. Mathematicians since Euclid have studied the properties of the golden ratio, including its appearance in the dimensions of a regular pentagon and in a golden rectangle, which can be cut into a square and a smaller rectangle with the same aspect ratio.)

5.2 For the recursively defined sequences (a_n) in the parts (a) ,(b) ,(c) below, prove the given explicit representations.

(a) $a_0 = 2$, $a_n = 2 - a_{n-1}^{-1}$, $n \geq 1$. Then $a_n = (n+2)/(n+1)$ for all $n \in \mathbb{N}$.

(b) $a_0 = 0$, $a_1 = 1$, $a_n = \frac{1}{2}(a_{n-1} + a_{n-2})$, $n \geq 2$. Then $a_n = \frac{2}{3}\left(1 - (-1)^n \frac{1}{2^n}\right)$ for all $n \in \mathbb{N}$.

(c) $a_0 = 1$, $a_n = 1 + a_{n-1}^{-1}$, $n \geq 1$. Then $a_n = f_{n+2}/f_{n+1}$ for all $n \in \mathbb{N}$, where for $k \in \mathbb{N}$, f_k is the k-th Fibonacci-number (see Exercise 5.1).

(d) $a_0 = 1$, $a_n = \sum_{k=0}^{n-1} a_k$, $n \geq 1$. Then $a_n = 2^{n-1}$ for all $n \geq 1$.

5.3 The notion of greatest common divisor (see T5.14) can be extended to more than two integers in an obvious way. Let $a_1, \ldots, a_n \in \mathbb{N}$, $n \geq 1$, not all zero. Then $\gcd(a_1, \ldots, a_n)$ is defined to be the positive integer d satisfying the following two properties : (i) $d \mid a_i$ for every $i = 1, \ldots, n$; (ii) if c is a positive integer with $c \mid a_i$ for every $i = 1, \ldots, n$, then $c \mid d$ (or, equivalently $c \leq d$).

[4]The number of petals in a flower consistently follows the Fibonacci sequence. Famous examples include the lily.

[5]This shape, a rectangle in which the ratio of the sides is equal to the golden mean, can result in a nesting process that can be repeated into infinity — and which takes on the form of a spiral. It is called the *logarithmic spiral*, and it abounds in nature.

[6]The mouth and nose are each positioned at golden sections of the distance between the eyes and the bottom of the chin. Similar proportions can been seen from the side, and even the eye and ear itself.

Note that $\gcd(a_1,\ldots,a_{n-1},a_n) = \gcd(\gcd(a_1,\ldots,a_{n-1}),a_n) = \cdots = \gcd(a_1,\gcd(a_2,\ldots,a_n))$ by T5.14-(b)-(iv) and hence the gcd depends only on $a_1,\ldots,a_n$ and not on the order in which they are written. Similarly, the notion of least common multiple (see T5.15) can be extended to more than two integers in an obvious way.

(a) Let $a_1,\ldots,a_n \in \mathbb{N}^*$, $n \geq 1$ and let $a = a_1 \cdots a_n$. Show that the following statements are equivalent:

(i) $a_1,\ldots,a_n$ are pairwise relatively prime.

(ii) If each $a_1,\ldots,a_n$ divide the natural number c, then a also divide the number c.

(iii) $\mathrm{lcm}(a_1,\ldots,a_n) = a$.

(iv) The natural numbers $b_1 := a/a_1,\ldots,b_n := a/a_n$ are relatively prime.

(v) There exist integers $s_1,\ldots,s_n$ such that $\dfrac{1}{a} = \dfrac{s_1}{a_1} + \cdots + \dfrac{s_n}{a_n}$.

(**Remark :** If $\gcd(a_1,\ldots,a_n) = 1$, then $a_1,\ldots,a_n$ are called relatively prime. Note that this concept is different from that of pairwise relatively prime.)

(b) For $a_1,\ldots,a_n \in \mathbb{N}^*$, $n \geq 1$, show that there exist $u_1,\ldots,u_n \in \mathbb{Z}$ such that $\gcd(a_1,\ldots,a_n) = u_1a_1 + \cdots + u_na_n$. In particular, $a_1,\ldots,a_n$ are relatively prime if and only if there exist integers $u_1,\ldots,u_n$ such that $1 = u_1a_1 + \cdots + u_na_n$. (**Remark :** One can find the coefficients $u_1,\ldots,u_n$ algorithmically by successive use of the lemma of Bezout (see T5.14-(a)). This algorithm supplies frequently disproportionately large coefficients $u_1,\ldots,u_n$. It is better to proceed as follows : First by renumbering assume that a_1 is minimal in $\{a_1,\ldots,a_n\}$, and goes then to tuple $(a_1,r_2,\ldots,r_n)$, where r_j the remainder of a_j after dividing by a_1, after removing the zeros among r_j, consider the new tuple as at the beginning. One has to control, how the coefficients of the tuple constructed are represented as linear combinations of the $a_1,\ldots,a_n$, beginning with $a_i = \sum_{k=1}^{n} \delta_{ik}a_k$.) Find integers u_1,u_2,u_3 such that $1 = u_1 \cdot 88 + u_2 \cdot 152 + u_3 \cdot 209$.

5.4 Let $(f_n)_{n\in\mathbb{N}}$ denote the Fibonacci sequence (see Exercise 5.1).

(a) For $m,n \in \mathbb{N}^*$, show that f_m divides f_{mn}. (**Hint :** Use Exercise T5.1-(b)-(i) and induction on n.)

(b) $\gcd(f_{n+2},f_{n+1}) = 1$. (**Hint:** The Euclidean Algorithm for obtaining the gcd leads to the system of n equations: $f_{n+2} = 1 \cdot f_{n+1} + f_n$; $f_{n+1} = 1 \cdot f_n + f_{n-1}$; $\cdots$ $f_3 = f_2 + f_1$ $f_2 = 2 \cdot f_1$.)

(c) $\gcd(f_m,f_n) = f_{\gcd(m,n)}$. (**Hint :** If $m = qn + r$, then $gcd(f_m,f_n) = \gcd(f_{qn-1}f_r + f_{qn}f_{r+1},f_n)$ by Exercise 5.1-(b)-(i). Further, since f_m divides f_{mn} by (a), it follows (by using $\gcd(a+c,b) = \gcd(a,b)$ if $b|c$) that $\gcd(f_{qn-1}f_r + f_{qn}f_{r+1},f_n) = \gcd(f_{qn-1}f_r,f_n) = 1$. For the last equality use parts (a) and (b).)

(d) The converse of (a) — For $n \geq m \geq 3$, if f_m divides f_n, then m divides n. (**Hint :** Use part (c). — **Remark :** It is interesting to note that: *For a prime number $p > 5$, either p divides f_{p-1} or p divides f_{p+1}, but not both.* The proof of this statement involves well known *Quadratic Reciprocity Law* due to Gauss.)

5.5 Let $\mathbb{P}$ denote the set of all prime numbers. Let p_n denote the n-th prime (in the natural order $\leq$ on $\mathbb{N}^*$, i. e. starting with $n = 1,2,\ldots,$). Then show that :

(a) $p_n > 2n-1$ for $n \geq 5$ and $p_n \leq 2^{2^{n-1}}$ for all $n \in \mathbb{N}^*$. (**Hint :** Note that $p_{n+1} \leq p_1 \cdot p_2 \cdots p_n + 1$.)

(b) None of the natural number $P_n := p_1 \cdot p_2 \cdots p_n + 1$ is a perfect square. (**Hint :** Each P_n is of the form $4m+3$.)

(c) The sum $\dfrac{1}{p_1} + \dfrac{1}{p_2} + \cdots + \dfrac{1}{p_n}$ is never an integer.

(d) Another proof of infiniteness of $\mathbb{P}$: Suppose that there are only finitely many primes, say, $p_1,\ldots,p_n$. Now, use the natural number $N = p_2 \cdot p_3 \cdots p_n + p_1 \cdot p_3 \cdots p_n + \cdots + p_2 \cdot p_3 \cdots p_{n-1}$.

5.6 (Gödelisation) Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ... be (infinite) sequence of the prime numbers.

(a) Let A be a countable set with an enumeration $A = \{a_1, a_2, a_3, \ldots\}$, $a_i \neq a_j$ for $i \neq j$. Then the map $(a_{i_1}, \ldots, a_{i_n}) \mapsto p_1^{i_1} \cdots p_n^{i_n}$ is an injective map from the set $\mathrm{W}(A) := \biguplus_{n \in \mathbb{N}} A^n$ of finite sequences (of arbitrary lengths) of elements from A - such sequences are also called w o r d s over the a l p h a b e t A - into the set $\mathbb{N}^*$ of positive natural numbers. (**Remark :** Such a coding of the words over A is called a G ö d e l i s a t i o n (due to K. Gödel[7]). The natural number associated to a word is called the G ö d e l n u m b e r of this word.)

(b) Let A be a finite alphabet $\{a_1, a_2, \ldots, a_g\}$ with g letters, $g \geq 2$, and $a_0 \notin A$ be another letter. A word $W = (a_{i_1}, \ldots, a_{i_n})$ over A can be identified by filling a_0 with the infinite sequence $(a_{i_1}, \ldots a_{i_n}, a_0, a_0, \ldots)$. Show that: the map $(a_{i_\nu})_{\nu \in \mathbb{N}^*} \mapsto \sum_{\nu=1}^{\infty} i_\nu g^{\nu-1}$ is a bijective map from the set of words over A onto the set $\mathbb{N}$ of the natural numbers and in particular, is a Gœdelisation. (**Remark :** This is a variant of the g-adic expansion (see T5.25).)

5.7 Let $g \in \mathbb{N}^*$, $g \geq 2$, n be a natural number with digit-sequence $(r_i)_{i \in \mathbb{N}}$ in the g-adic expansion of n and let $d \in \mathbb{N}^*$. (see T5.25.)

(a) Suppose that d is a divisor of g^α for some $\alpha \in \mathbb{N}^*$. Then $n \equiv (r_{\alpha-1}, \ldots, r_0)_g \bmod d$. In particular, d divides the number n if and only if d divides the number $(r_{\alpha-1}, \ldots, r_0)_g$.

(b) Suppose that d is a divisor of $g^\alpha - 1$ for some $\alpha \in \mathbb{N}^*$ and

$$S := (r_{\alpha-1}, \ldots, r_0)_g + (r_{2\alpha-1}, \ldots, r_\alpha)_g + \cdots .$$

Then $n \equiv S \bmod d$. In particular, d divides the number n if and only if d divides the sum S.

(c) Suppose that d is a divisor of $g^\alpha + 1$ for some $\alpha \in \mathbb{N}^*$ and

$$W := (r_{\alpha-1}, \ldots, r_0)_g - (r_{2\alpha-1}, \ldots, r_\alpha)_g + \cdots .$$

Then $n \equiv W \bmod d$. In particular, d divides the number n if and only if d divides the alternating sum W. (**Remark :** With the help of this exercise one can find criterion, which one can decide on the basis the digit-sequence of the natural number n in the decimal system whether d is a divisor of n with $2 \leq d \leq 16$. (with $d = 3$ and $d = 9$ one uses the simple check-sum, with $d = 11$ the simple alternating sum. The divisibility by $7, 11$ and 13 at the same time can be tested with the alternating sum of the 3-grouped together in view of the part (c). See T5.25-(d) for details.)

5.8 Let $n \in \mathbb{N}^*$. Show that :

(a) If $n > 1$ and if n divides $(n-1)! + 1$, then n must be a prime number.

(b) If $n > 2$, then there exists a prime number p with $n < p < n!$. (**Hint :** Consider a prime divisor p of $n! - 1$.)

(c) If $n > 1$, then every prime divisor of $n! + 1$ is an odd integer $> n$. (**Remark :** This shows again that there are infinitely many prime numbers. It is unknown whether infinitely many of $n! + 1$ are prime.)

(d) None of the n natural numbers $(n+1)! + 2, \ldots, (n+1)! + n + 1$ are prime. (**Remark :** Therefore there are gaps of any size between prime numbers.)

(e) Let $n, r \in \mathbb{N}^*$, $n \geq 2$. If n has no prime divisor $\leq \sqrt[r+1]{n}$, then n is a product of at the most r (not necessarily different) prime numbers. In particular, if n has no prime divisor $\leq \sqrt{n}$, then n is prime.

(f) For $n \in \mathbb{N}$, $n \geq 2$, the natural number $4^n + n^4$ is never prime. (**Hint :** For odd n, we have $n^4 + 4^n = (n^2 - 2^{\frac{n+1}{2}} \cdot n + 2^n)(n^2 + 2^{\frac{n+1}{2}} \cdot n + 2^n)$.)

5.9 (P e r i o d i c S e q u e n c e s) Let us fix the terminology for periodic sequences which is used at many places: For an arbitrary sequence $(x_i)_{i \in \mathbb{N}}$ of elements of a set X, a pair $(m_0, n) \in$

[7] K u r t G ö d e l (1906-1978) was born on 28 April 1906 in Brünn, Austria-Hungary (now Brno, Czech Republic) and died on 14 Jan 1978 in Princeton, New Jersey, USA. Gödel proved fundamental results about axiomatic systems showing in any axiomatic mathematical system there are propositions that cannot be proved or disproved within the axioms of the system.

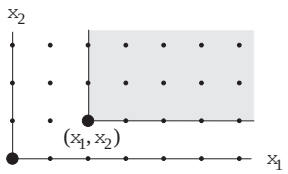
$\mathbb{N}\times\mathbb{N}^*$ is called a pair of periodicity for (x_i) if $x_{i+n}=x_i$ for all $i\geq m_0$. In this case m_0 is called a pre-period length and n a period length of (x_i). If no such pair of periodicity for (x_i) exists, then (x_i) is called aperiodic, otherwise (x_i) is called periodic.

(a) Show that for a periodic sequence $(x_i)_{i\in\mathbb{N}}$, there exists a *unique* pair of periodicity $(k_0,\ell)\in\mathbb{N}\times\mathbb{N}^*$ with the following property: Any pair of periodicity for (x_i) is of the form $(m_0,m\ell)$ with $m_0\geq k_0$ and $m\in\mathbb{N}^*$. (**Hint :** The main point to show is the following: If $r,s\in\mathbb{N}^*$ are period lengths of (x_i), then $\mathrm{GCD}(r,s)$ is also a period length of (x_i).) – The natural number k_0 is called *the* pre-period length of (x_i) and the natural number ℓ is called *the* period length. The pair (k_0,ℓ) itself is called the (periodicity) type of (x_i). The (finite) subsequence $(x_0,\ldots,x_{k_0-1})$ is called *the* pre-period of (x_i) and the (finite) subsequence $(x_{k_0},\ldots,x_{k_0+\ell-1})$ is called *the* period of (x_i). In this case we simply write $(x_i)_{i\in\mathbb{N}}=(x_0,\ldots,x_{k_0-1},\overline{x_{k_0},\ldots,x_{k_0+\ell-1}})$. If $k_0=0$ then (x_i) is called purely periodic. The periodicity type of an aperiodic sequence is often denoted by $(\infty,0)$. In particular, by definition, the period length of an aperiodic sequence is 0.

(b) If x is an element of a group, the sequence $(x^i)_{i\in\mathbb{N}}$ of its powers has period length $\mathrm{ord}\,x$ and is purely periodic if $\mathrm{ord}\,x>0$. For an element x of a monoid the periodicity type of the sequence $(x^i)_{i\in\mathbb{N}}$ characterizes the cyclic monoid generated by x up to isomorphism and any type in $\mathbb{N}\times\mathbb{N}^*\cup\{(\infty,0)\}$ may occur.

(c) For an integer $r\in\mathbb{N}^*$, compute the periodicity type of the sequence $(x_{ri})_{i\in\mathbb{N}}$ in terms of the periodicity type (k_0,ℓ) of $(x_i)_{i\in\mathbb{N}}$.

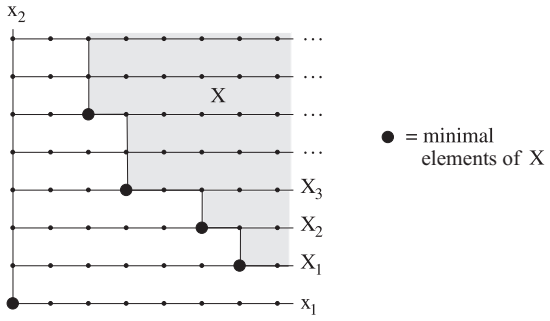
***5.10** (Dickson's Lemma[8]) Let $r\in\mathbb{N}^+$. The set $\mathbb{N}^r=\mathbb{N}\times\cdots\times\mathbb{N}$ (r-times) of the r-tuples of natural numbers is ordered by the product order of the usual order on $\mathbb{N}$, i. e. by definition $(x_1,\ldots,x_r)\leq(y_1,\ldots,y_r)$ if and only if $x_i\leq y_i$ for all $i=1,\ldots,r$. For $r\geq 2$, this product order is not a total order. For $r=2$, the set of points $\geq(x_1,x_2)$ is shaded in the following picture:



Sketch the picture for the set of points $\leq(x_1,x_2)$. Clearly $(0,\ldots,0)\in\mathbb{N}^r$ is the least element of $\mathbb{N}^r$. Let X be an arbitrary subset of $\mathbb{N}^r$ (with the induced order from the product order of $\mathbb{N}^r$). Show that X has only finitely many minimal elements. (**Hint :** Proof by induction on r. For this one may assume that if a r-tuple $x\in X$, then all r-tuples $y\in\mathbb{N}^r$ with $x\leq y$ also belong to X. This means replace X by the set $\bigcup_{x\in X}(x+\mathbb{N}^r)$. Note that this does not change the set of minimal elements. For the inductive step from r to $r+1$, apply induction-hypothesis to the sets $X'_n:=\{x'\in\mathbb{N}^r\mid(x',n)\in X\}\subseteq\mathbb{N}^r$, $n\in\mathbb{N}$. Observe that $X'_0\subseteq X'_1\subseteq X'_2\subseteq\cdots$ and there exists $n_0\in\mathbb{N}$ such that $X'_n=X'_{n_0}$ for all $n\geq n_0$. This already proves the case from $r=1$ to $r+1=2$:

---

[8]This simple fact from combinatorics has become attributed to the American algebraist L. E. Dickson (1874-1954), who used it to prove a result in number theory about *perfect numbers*. He was one of the first American researchers in abstract algebra, in particular the theory of finite fields and classical groups, and is also remembered for a three-volume history of number theory, History of the Theory of Numbers. However, the lemma was certainly known earlier, for example to Paul Gordan in his research on *invariant theory*. Paul Albert Gordan (1837-1912) was a German mathematician, a student of Carl Jacobi at the University of Königsberg before obtaining his Ph.D. at the University of Breslau (1862), and a professor at the University of Erlangen-Nuremberg. He was known as "the king of invariant theory". Gordan also served as the thesis advisor for Emmy Noether.
The tuples $(a_1,a_2,\ldots,a_n)in\mathbb{N}^n$ are in bijective correspondence with the monomials $X_1^{a_1}X_2^{a_2}\ldots X_n^{a_n}$ over a set of n variables $X_1,X_2,\ldots X_n$. Under this correspondence, Dickson's lemma may be seen as a special case of the *Hilbert's basis theorem* which states that: *every polynomial ideal generated by monomials has a finite basis.* Indeed, Paul Gordan used this restatement of Dickson's lemma in 1899 to prove the Hilbert's basis theorem.



and makes it clear how can one make a general argument.)

R **5.11** Congruences (see T5.24) are often used to append extra check digit to identification numbers, in order to recognize transmission errors or forgeries. Personal identification numbers of some kind on passports, credit cards, bank accounts and other variety of settings.

(a) Some banks use eight digit identification number $a_1a_2\cdots a_8$ together with a final check digit a_9. The check digit is the weighted sum of the eight modulo 10, i. e. $a_9 \equiv \sum_{i=1}^{8} x_i a_i \pmod{10}$.

Suppose that $a_9 \equiv 7a_1+3a_2+9a_3+7a_4+3a_5+9a_6+7a_7+3a_8 \equiv \pmod{10}$. Then:

(i) Verify that the identification number 815042169 have the check digit 9. Obtain the check digits that should be appended to the numbers 55382006 and 81372439.

(ii) The weighting scheme for assigning check digit detects any single-digit error[9] in the identification number. For example, suppose that the digit a_i is replaced by a different digit a_i', then the difference between the correct a_9 and the new check digit a_9' is $a_9 - a_9' \equiv k(a_i - a_i') \pmod{10}$, where $k = 7, 3$, or 9 depending position of a_i'. If the valid number is 81504216 were incorrectly entered as 81504316, then the check digit 8 would come up rather than the expected 9.

(iii) The bank identification number $237a_418538$ has an illegible fourth digit. Determine the value of the obscured digit.

(b) The International Standard Book Number (ISBN) used in many libraries consist of none digits $a_1a_2\cdots a_8a_9$ followed by a tenth check digit a_{10} which satisfies $a_{10} \equiv \sum_{i=1}^{9} i \cdot a_i \pmod{10}$. Determine whether each of the ISBNs below correct:

(i) 0-07-232569-0 (United States) (ii) 91-7643-497-5 (Sweden) (iii) 1-56947-3034-10 (England).

When printing the ISBN $a_1a_2\cdots a_8a_9$ two unequal digits were transposed. Show that the check digits detected this error.

Below one can see Lecture Notes.

[9] The modulo 10 approach is not entirely effective. For, it does not always detect the common error of transposing distinct adjacent entries a and b within the string of digits. For example, the identification numbers 81504216 and 81504261 have the same check digit 9. The problem occurs when $|a-b| = 5$. More sophisticated methods are available with larger moduli and different weights that would prevent this error.