Hugo *Rincon Galeana*

TU Wien, Winter 2019
104.272 Discrete Mathematics, Group 1 (Professor Gittenberger)
10. Exercise, Due 8 January, 2020

91. Let (e, n) and (d, n) be Bob's public and private RSA keys, respectively. Suppose that Bob sends an encrypted message c and Alice wants to find out the original message m. She has the idea to send Bob a message and ask him to sign it. How can she find out m?

    Hint: Pick a random integer r and consider the message $r^e c \bmod n$. What property does r need to satisfy?

    Proof. Notice that $c \underset{\text{mod } n}{\equiv} m^e$. First we apply the Euclidian algorithm in order to find $\gcd(c, n)$. Notice that if $\gcd(c, n) \neq 1$, then $\gcd(c, n)$ is one of the prime factors, and we can obtain the private key.

    If c is a unit in $\mathbb{Z}_n$, then we test $r^e c = r^e m^e$. Notice that if $r^e m^e \underset{\text{mod } n}{\equiv} 1$, then r is the product inverse of m in $\mathbb{Z}_n$. Therefore it suffices to invert r modulo n via the Euclidian algorithm in order to obtain m.

    Notice that this attack is impractical for a sufficiently large n since it requires encrypting and multiplying for a large amount of numbers. Namely for $p \cdot q - (q + p - 1)$. □

92. Let G be a finite (abelian) group and $a \in G$ an element for which $\text{ord}_G(a)$ is maximal. Prove that for all $b \in G$, the order $\text{ord}_G(b)$ is a divisor of $\text{ord}_G(a)$.

    Proof. Notice that it is important that G is abelian, otherwise S_3 is an example of a non-abelian group in which the order of any 3-cycle is 3, the order of any 2-cycle is 2, and the identity permutation is of order 1. Therefore, an element of max order is of order 3, however a 2-cycle is of order 2 which does not divide 3.

    Assume for a contradiction that $\text{ord}_G(b) \nmid \text{ord}_G(a)$. From a previous theorem, there must exist $c \in G$ such that $\text{ord}_G(c) = \text{lcm}(\text{ord}_G(a), \text{ord}_G(b))$. Since a is of maximal order in G, then $\text{ord}_G(a) \leq \text{lcm}(\text{ord}_G(a), \text{ord}_G(b)) \leq \text{ord}_G(a)$. This implies that $\text{ord}_G(a)$ is a multiple of $\text{ord}_G(b)$.

    This is a contradiction. □

93. Prove that if G is a finite group and $a \in G$ is an element with $\text{ord}_G(a) = r$, then for every $k \in \mathbb{N}$, $\text{ord}_G(a^k) = r/\gcd(r, k)$.

    Proof. Let $c := a^k$. Notice that $c^{r/\text{gcd(r,k)}} = a^{k \cdot r/\text{gcd}(r,k)} = a^{lcm(r,k)} = e$.

    Therefore $\text{ord}_G(c) \mid r/\gcd(r, k)$.

Also since $\text{ord}_G(a^k) := m$ is the smallest positive integer such that $(a^k)^m = e$, then $a^{k\cdot m} = e$, then $k \cdot m$ is a multiple of r, in fact $k \cdot m = \text{lcm}(k, r)$, otherwise $\text{lcm}(k, r) = k \cdot m'$ with $m' < m$, thus $a^{k\cdot m'} = e$, therefore $c^{m'} = e$, contradicting that $\text{ord}_G(c) = m$.

Now notice that $k \cdot m = \text{lcm}(k, r) = k \cdot r/\gcd(k, r)$. Therefore $m = r/\gcd(k, r)$. □

94. Use the Euclidean algorithm to find all greatest common divisors of $x^3 + 5x^2 + 7x + 3$ and $x^3 + x^2 - 5x + 3$ in $\mathbb{Q}[x]$.

Proof.
$$\begin{array}{rrrl} x^3 & +5x^2 & +7x+3 & = \left(x^3+x^2-5x+3\right)1 + 4x^2 + 12x \\ \underline{-x^3} & \underline{-x^2} & \underline{+5x-3} & \\ & & 4x^2+12x & \end{array}$$

$$\begin{array}{rrrl} x^3 & +x^2 & -5x+3 & = \left(x^2+3x\right)\left(x-2\right) + x + 3 \\ \underline{-x^3} & \underline{-3x^2} & & \\ & -2x^2 & -5x & \\ & \underline{2x^2} & \underline{+6x} & \\ & & x & \end{array}$$

$$\begin{array}{rrl} x^2 & +3x & = \left(x+3\right)x \\ \underline{-x^2} & \underline{-3x} & \\ & 0 & \end{array}$$

This shows that $x + 3 = \gcd(p(x), q(x))$ □

95. Prove that $x^4 + x^3 + 1$ is irreducible over $\mathbb{Z}_2$.

Proof. Notice that evaluating $p(0) = 1 = p(1)$. Therefore $p(x)$ doesn't have factors of degree 1, and therefore no factors of degree 3.

Let us consider a polynomial $q(x)$ of degree 2. Notice also that in $\mathbb{Z}_2$ the following equation holds $x^2 = x$. Therefore any polynomial of degree 2 in $\mathbb{Z}_2, x^2 + ax + b$ has the same root as $(1 + a)x + b$. Notice that if $b = 0$ then $q(x)$ has a root. Also if $b = 1$ and $a = 0$, then it also has a root. Therefore $q(x) = x^2 + x + 1$ is the only polynomial of degree 2 without a root in $\mathbb{Z}_2$.

This means that $q(x)$ is the only viable candidate for being a factor of $p(x)$, since the rest of the polynomials imply the existence of at least one root. However $(x^2 + x + 1)^2 = x^4 + x^3 + x^2 + x^3 + x^2 + x + x^2 + x + 1 = x^4 + x^2 + 1 \neq p(x)$.

Therefore $p(x)$ is irreducible. □

96. List all irreducible polynomials up to degree 3 in $\mathbb{Z}_3$ Since $\mathbb{Z}_3$ is a field, we will only consider irreducible polynomials with main coefficient 1.

We start with the polynomials of degree 1

$$x, x+1, x+2$$

.

We proceed with the polynomials of degree 2.

Notice that a polynomial of degree 2 is irreducible if and only if it does not have a root. Notice that the independent term should be different than 0 in order to avoid the root 0.

We test the polynomials and we obtain

$$x^2+1; x^2+x+1$$
$$x^2+x+2; x^2+2x+2$$

Now, for the polynomials of degree 3 we notice that in $\mathbb{Z}_3$, $x^3 = x$. Since a non reducible polynomial of degree 3 may always be factored by a polynomial of degree 1, it is sufficient to show that it doesn't have a root in order to show that it is irreducible.

Also notice from the first observation that $p(x) = x^3 + a_2x^2 + a_1x + a_0$ is irreducible if and only if $a_2x^2 + (a_1+1)x + a_0$ is irreducible.

We now proceed to find all irreducible monic polynomials of degree 3 by using the list of monic polynomials of degree 2.

x^2+1 yields x^3+x^2+2x+1 and x^3+2x^2+2x+2

x^2+x+1 yields x^3+x^2+1 and x^3+2x^2+x+2

x^3+x^2+2 yields x^3+x^2+2 and x^3+2x^2+x+1

x^2+2x+2 yields x^3+x^2+x+2 and x^3+2x^2+1

97. Let $\mathbb{K}$ be a field and $p(x) \in \mathbb{K}[x]$ a polynomial of degree m. Prove that $p(x)$ cannot have more than m zeroes (counted with multiplicities). *Hint: Use the fact that $\mathbb{K}[x]$ is a factorial ring.*

Proof. Assume by contradiction that $p(x)$ has at least $m+1$ roots.

Consider the following sequences of roots $(r_1, \ldots, r_m)$ and $(r_1, \ldots, r_{m-1}, r_{m+1})$. Notice that the first sequence yields the factorization $(x-r_1)(x-r_2)\ldots(x-r_m)$ for $p(x)$. The second sequence yields the factorization $(x-r_1)\ldots(x-r_{m-1})(x-r_{m+1})$. This contradicts the fact that $\mathbb{K}[x]$ is a factorial ring. □

98. Let R be a ring and $(I_j)_{j\in J}$ be a family of ideals of R. Prove that $\bigcap_{j\in J} I_j$ is also an ideal of R.

Proof. Notice that since each of the I_j is an ideal, then $0 \in I_j, \forall j \in J$. Therefore $0 \in \bigcap_{j\in J} I_j$. Thus $\bigcap_{j\in J} I_j \neq \varnothing$.

Let $x, y \in \bigcap_{j\in J} I_j$. Let I_j be an ideal of the family, it follows that $x, y \in I_j$, therefore $x - y \in I_j$ for all $j \in J$. Therefore $x - y \in \bigcap_{j\in J} I_j$.

Let $a \in R$ and $i \in \bigcap_{j\in J} I_j$. Since each of the I_j are ideals of R, then $a \cdot i \in I_j$. Therefore $a \cdot i \in \bigcap_{j\in J} I_j$.

Therefore $\bigcap_{j\in J} I_j$ has all the properties of an ideal of R. □

99. Let R be a ring and I an ideal of R. Then $(R/I, +)$ is the factor group of $(R, +)$ over $(I, +)$. Define a multiplication on R/I by

$$(a + I) \cdot (b + I) := (ab) + I.$$

Prove that this operation is well defined, i.e. that

$$a + I = c + I \wedge b + I = d + I \Rightarrow (ab) + I = (cd) + I.$$

Furthermore, show that $(R/I, +, \cdot)$ is a ring.

Proof. Assume that $a + I = c + I \wedge b + I = d + I$.

Then $a = c + i_1$ for some $i_1 \in I$, $b = d + i_2$ for some $i_2 \in I$.

Consider $ab = (c + i_1) \cdot (d + i_2) = cd + ci_2 + di_1 + i_1i_2$. Since $i_1, i_2 \in I$, then $ci_2, di_1, i_1i_2 \in I$. Since I is an ideal, it is also closed under sums, therefore $ci_2 + di_1 + i_1i_2 = i_3 \in I$. Therefore $ab = cd + i_3$ for some $i_3 \in I$. this shows that $ab + I = cd + I$.

Notice that the 0 element is given by I, the e-element is given by $e + I$.

Also notice that the additive inverse of $a + I$ is given by $-a + I$.

Consider $((a + I)(b + I))c + I = (ab + I)(c + I) = (ab)c + I = a(bc) + I = a + I((b + I)(c + I))$. This shows the associative property of the product.

Now consider $(a + I + b + I)(c + I) = (a + b + I)(c + I) = (a + b)c + I = ac + bc + I = ac + I + bc + I$. This shows the distributive property of the product (analogous for the left distributivity).

□

100. Let $U = \{\bar{0}, \bar{2}, \bar{4}\} \subseteq \mathbb{Z}_6$. Show that U is an ideal of $(\mathbb{Z}_6, +, \cdot)$. Is it a subring as well? Does it have a 1-element?.

Proof. Notice that U are the even numbers of $\mathbb{Z}_6$. Since 6 is also even, then for any $z \in \mathbb{Z}_6$ and any $u \in U$, $zu \in U$. Notice that U is closed under addition and under additive inverse since $-\bar{0} = \bar{0}$ and $-\bar{2} = \bar{4}$. Therefore it is closed under subtraction.

Therefore it is an ideal of $\mathbb{Z}_6$. Since it is an ideal, it is also a subring. Notice that $\bar{4}$ is the 1-element of U. □