## 6.3 Residue Class Rings

n ∈ ℕ with . We have already discussed in detail the congruent modulus equiva- with respect to . We have seen that ∼n. On this basis,ℤ = through the use of codes.cryptography is a method cryptography. Cryptography Literally “hidden writing”,

Let of protecting information

Definition: ℤ modulo nℤ Let n be ∈ ℕ be the congruent modulo equivalence relation. Thenℤ/nℤ ℤ modulo nℤ.

we define . is read “ ”

ℤ/nℤ 01 ==

Based on this definition, we want to define the residue class ring. This plays a decisive roleExample: The elements of the set 2.1. ℤ/12ℤℤ/2ℤ forms the two equivalence classesℤ forms the twelve equivalence classes modulo nℤ10106870123459==============…, ‐6, ‐4, ‐2, 0, 2, 4, 6,…, ‐5, ‐3, ‐1, 1, 3, 5, ……, ‐18, ‐6, 6, 18, 30, ……, ‐13, ‐1, 11, 23, 35, ……, ‐14, ‐2, 10, 22, 34, …, ‐15, ‐3, 9, 21, 33, ……, ‐16, ‐4, 8, 20, 32, ……, ‐22, ‐10, 2, 14, 26, …, ‐23, ‐11, 1, 13, 25, ……, ‐17, ‐5, 7, 19, 31, ……, ‐21, ‐9, 3, 15, 27, ……, ‐20, ‐8, 4, 16, 28, ……, ‐19, ‐7, 5, 17, 29, ……, ‐24, ‐12, 0, 12, 24, … are therefore the n−1 =⋮ n1+0+−knkn1+nkk disjoint residue classeskn∈∈ ………ℤℤk ∈ ℤ

11

in cryptography.

tient ring.For and Then Theorem and Definition: Residue Class Ring[·:a], [b] ∈ ℤ/nℤ ℤ/nℤ × → ℤ /nℤ → ℤ/nℤ(ℤ/nℤ, +, ·) is a commutative ring. This ring is called a residue class ring or a quo- is + : ℤ/nℤ × ℤ/nℤ →ℤ/nℤ defined byaa+· bb ∶∶ == a+ba·b is defined by

Proof:

must be well defined, i.e., the results of the operations must be independent of the con-=Let us first prove the well-defined nature of addition:First we have to show that crete choice of the representatives of [b′], [a + b] = [a′ + b′] and + and [a · b] = [a′ · b′· are actually links on [a] and [b]]. We must show that for . ℤ/nℤ. For this purpose,

Because thus The addition is thus defined independently of the concrete choice of the representativesb ∼a′) + (b − b′) = (a + b) − (a′ + b′)n b′ n (a′ + b′) is n|(b − b′). It is therefore a′ and therefore . Thus it follows in total that [n|(a − a′) + (b − b′)a + b] = [a′ + b′n|(a − a′). Accordingly, because of ]. n|(a + b) − (a′ + b′) applies. Because of [b] = [b′( anda −],

of the equivalence classes and thus well defined.

(

a′ · b′The multiplication is thus also independent of the concrete choice of representatives and+The well-defined nature of multiplication is shown in a very similar way:a − a′) · b = a · b − a′ · b (a′ · b − a′ · b′) = a · b − a′· b′ and thus n|(a′ ·b − a′ · b′)[a · b] = [a′ · b′. Thus it applies that and . Thus ] it follows with the same argumentation as above that . (b − b′) · a′ = a′ · b − a′ · b′, i.e., n in particular also divides the sum n|(a · b − a′ · b′)n|(a − a′) · b and . From this follows n|(b − b′) · a it applies that (a · b − a′ · b. Because ofa · b ∼n|(a · bn|)n

properties of rings and the commutative law apply, i.e., we must show the following:thus well defined.All in all, + and · are therefore operations on ℤ/nℤ. It remains to be shown that the three 1.2.3. (the distribution laws for rings apply to all ℤ/nℤ, +) is commutative. is a semigroup with a neutral element. is an abelian group. a, b, c ∈ ℤ/nℤ

(The addition is therefore associative.Let ℤ, [+)a], [b], [c] ∈ ℤ/nℤ the associative law applies, the following applies:. Then according to the above definition of addition and because ina + b + c ===== aaa+ba+ba+++bb+b+c+++cccc Furthermore it applies that:The addition is therefore also commutative.a + b === a+bb+ab + a

a + −a ==== a

(Two:each Because ofℤ/nℤ, [a] ∈ ℤ/nℤ+) is an abelian group. has an inverse element [−=a] ∈ ℤ /nℤ0−a+−−aaa+−+aaa with respect to + in ℤ/nℤ. Thus

Be The multiplication is therefore associative.[a], [b], [c]∈ ℤ/nℤ. Because in a (·ℤ, ·b)· the associative law appliesc ===== aaa·baa·b···bbb··c·c·c·cc

Furthermore, because ofit follows that [1] is the identity element regarding group with a neutral element. a · 1 ==== a·1a11·a· a · in ℤ/nℤ. Thus (ℤ/nℤ, ·) is a semifollowsTo 3.:Let [a], [b], [c] ∈ ℤ/nℤ. Because in (ℤ, +, ·) the distribution laws are valid, the following and a · b + c =====aa·a·a·ba ··bbb+a·cb+++c+a·cca · c

Thus, the distribution laws apply to rings.a + b · c ===== aa·caa+ba+b·c+b·c· c++·cb·c·bc · c

To 4.:Let it follows that commutativity applies.[a], [b] ∈ ℤ/nℤ. Because of a · b === a·bb·ab · a

Thus it follows that Example: residue class rings(ℤ/nℤ, +, ·) is a commutative ring. □

includes, for exampleWe consider (ℤ/2ℤ, +, ·). (ℤ/2ℤ, +, ·) is the smallest of all residue class rings. This

Consider twelfthdial of an analog clock. On such a clock, hours from one to twelve are written, the hour also being regarded as zero hour. Each hour on the clock thus corre-(ℤ/12ℤ, +, ·). Here one can illustrate the calculation in this ring with the17123+++·· 31843 ===== 924158=====00101 watch continues to move, add one or more hours, e.g., example, if you move five hours forward from 9 o’clock, the hand will then be at 2sponds to an equivalence class [11]. The hand may exceed the twelfth[0], [1], hour. Then it starts again in front at one. For., [11] with [12] = [0][4] + [1] = [5] o’clock. Because of [9] + [5] = [14] = [2] this corresponds exactly to the addition in lated as follows: [3] + [14] = [17] = [5]. The following figure illustrates the two calcuthe equivalence classes. Another example: If the hand is set to 3 o’clock and the time is advanced by 14 hours, the hand will then move to 5 o’clock. This can again be calcu-

lations once again graphically.

Figure 13: Addition in (ℤ/12ℤ, 12ℤ +, -): [9] + [5] = [2] (left) and [3] + [14] = [5] (right)

R (ℤ, +, ·)