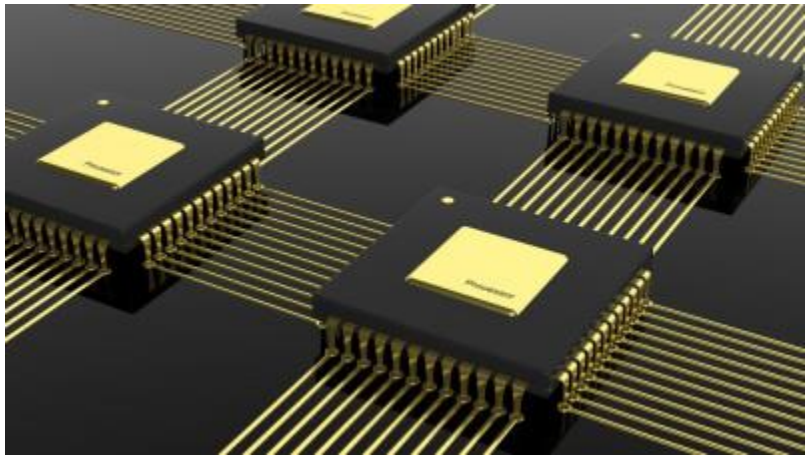
Lecture 13

Application (2)

*13.1 An Application to Parallel Computing (並列計算)

*13.2 Weird Dice: An Application of Unique Factorization



*13.1 An Application to Parallel Computing

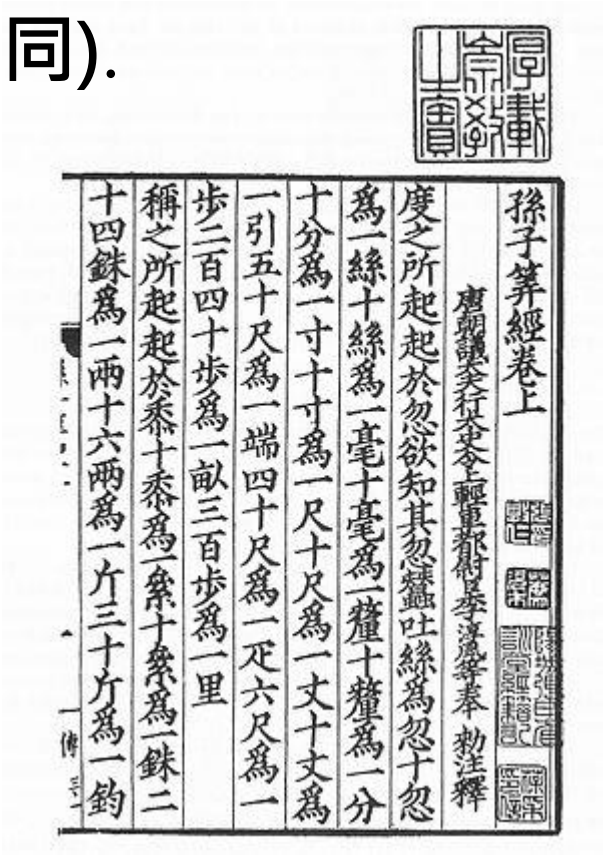
(並列計算)

*13.1 An Application to Parallel Computing (並列計算)

We here introduce **The Chinese Remainder Theorem (中国の剰余定理)** which is a result from elementary **number theory (数論)** about the solution of systems of **simultaneous congruences (合同)**.

The Chinese mathematician **Sun Zi** wrote about the theorem in **the** 3rd **century A.D.**

This theorem has some interesting consequences in the **efficient computation for parallel processors.**


孫子算經卷上

Lemma 13.1

Let m and n be positive integers such that $\gcd(m,n) = 1$. Then for $a, b \in \mathbb{Z}$ the system

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

has a solution. If x_1 and x_2 are two solutions of the system, then

$$x_1 \equiv x_2 \pmod{mn}$$

Proof

The equation $x \equiv a \pmod{m}$ has a solution since $a + km$ satisfies the equation for all $k \in \mathbb{Z}$. We must show that there exists an integer k_1 such that

$$a + k_1 m \equiv b \pmod{n}$$

This is equivalent to showing that

$$k_1 m \equiv (b - a) \pmod{n}$$

has a solution for k_1. Since m and n are relatively prime, there exist integers s and t such that $ms + nt = 1$.

*13.1 An Application to Parallel Computing (並列計算)

Proof (cont.)

Consequently,

$$(b-a)ms = (b-a)(1-nt) = (b-a) - (b-a)nt$$

or

$$[(b-a)s]m \equiv (b-a) \pmod{n}$$

Now let $k_1 = (b-a)s$.
To show that any two solutions are congruent modulo mn, let c_1 and c_2 be two solutions of the system. That is,

$$c_i \equiv a \pmod{m}$$
$$c_i \equiv b \pmod{n}$$

for $i = 1, 2$. Then

$$c_2 \equiv c_1 \pmod{m}$$
$$c_2 \equiv c_1 \pmod{n}$$

Therefore, both m and n divide $c_1 - c_2$. Consequently, $c_2 \equiv c_1 \pmod{mn}$.

*13.1 An Application to Parallel Computing (並列計算)

Example 13.1

Let us solve the system

$$x \equiv 3 \pmod{4}$$

$$x \equiv 4 \pmod{5}$$

Using the Euclidean algorithm, we can find integers s and t such that $4s + 5t = 1$. Two such integers are $s = 4$ and $t = -3$. Consequently,

$$x = a + k_1 m = 3 + 4k_1 = 3 + 4[(5 - 4)4] = 19$$

Theorem 13.1 (Chinese Remainder Theorem (中国の剰余定理))

Let $n_1, n_2, \ldots, n_k$ be **positive integers** such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then **for any integers** $n_1, a_2, \ldots, a_k$, **the system**

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a solution. Furthermore, **any two solutions of the system are congruent modulo** $n_1 n_2 \cdots n_k$.

Proof

We will use mathematical induction on the number of equations in the system. If there are $k = 2$ equations, then the theorem is true by Lemma 13.1. Now suppose that the result is true for a system of k equations or less and that we wish to find a solution of

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_{k+1} \pmod{n_{k+1}} \end{aligned}$$

Considering the first k equations, there exists a solution that is unique modulo $n_1 n_2 \cdots n_k$, say a. Since $n_1 n_2 \cdots n_k$ and n_{k+1} are relatively prime, the system

$$\begin{aligned} x &\equiv a \pmod{n_1 n_2 \cdots n_k} \\ x &\equiv a_{k+1} \pmod{n_{k+1}} \end{aligned}$$

has a solution that is unique modulo $n_1 n_2 \cdots n_{k+1}$ by the Lemma 13.1.

Example 13.2

Let us solve the system

$$x \equiv 3 \pmod 4$$
$$x \equiv 4 \pmod 5$$
$$x \equiv 1 \pmod 9$$
$$x \equiv 5 \pmod 7$$

From Example 13.1 we know that 19 is a solution of the first two congruences and any other solution of the system is congruent to $19 \pmod{20}$. Hence, we can reduce the system to a system of three congruences:

$$x \equiv 19 \pmod{20} \quad \text{(Here } 20 = 4 \cdot 5\text{)}$$
$$x \equiv 1 \pmod 9$$
$$x \equiv 5 \pmod 7$$

Solving the next two equations, we can reduce the system to

$$x \equiv 19 \pmod{180}$$
$$x \equiv 5 \pmod 7$$

Solving this last system, we find that

$$x \equiv 19 \pmod{1260} \quad \text{(Here } 1260 = 180 \cdot 7\text{)}$$

namely, 19 is a solution for the system that is unique up to modulo 1260.

*13.1 An Application to Parallel Computing (並列計算)

One interesting application of the **Chinese Remainder Theorem** in the design of computer software is that **the theorem allows us to break up a calculation involving large integers into several less formidable calculations**.

A computer will handle integer calculations only up to a certain size due to the size of its processor chip, **which is usually a 32 or 64-bit processor chip**.

For example, the largest integer available on a computer with a 64-bit processor chip is

$$2^{63} - 1 = 9{,}223{,}372{,}036{,}854{,}775{,}807$$

Larger processors such as 128 or 256-bit have been proposed or are under development. There is even talk of a 512-bit processor chip. The largest integer that such a chip could store with be $2^{511} - 1$, which would be a 154 digit number. However, we would need to deal with much larger numbers to break sophisticated encryption schemes.

*13.1 An Application to Parallel Computing (並列計算)

This is especially useful on parallel processing computers which have the ability to run several programs concurrently.

Most computers have a single central processing unit (CPU) containing one processor chip and can only add two numbers at a time. To add a list of ten numbers, the CPU must do nine additions in sequence. However, a parallel processing computer has more than one CPU. A computer with 10 CPUs, for example, can perform 10 different additions at the same time.

If we can take a large integer and break it down into parts, sending each part to a different CPU, then by performing several additions or multiplications simultaneously on those parts, we can work with an integer that the computer would not be able to handle as a whole.

*13.1 An Application to Parallel Computing (並列計算)

Example 13.3

Suppose that we wish to multiply 2134 by 1531. We will use the integers 95, 97, 98, and 99 because they are relatively prime. We can break down each integer into four parts:

$$2134 \equiv 44 \pmod{95}$$
$$2134 \equiv 0 \pmod{97}$$
$$2134 \equiv 76 \pmod{98}$$
$$2134 \equiv 55 \pmod{99}$$

and

$$1531 \equiv 11 \pmod{95}$$
$$1531 \equiv 76 \pmod{97}$$
$$1531 \equiv 61 \pmod{98}$$
$$1531 \equiv 46 \pmod{99}$$

Multiplying the corresponding equations, we obtain

$$2134 \cdot 1531 \equiv 44 \cdot 11 \equiv 9 \pmod{95}$$
$$2134 \cdot 1531 \equiv 0 \cdot 76 \equiv 0 \pmod{97}$$
$$2134 \cdot 1531 \equiv 76 \cdot 61 \equiv 30 \pmod{98}$$
$$2134 \cdot 1531 \equiv 55 \cdot 46 \equiv 55 \pmod{99}$$

Example 13.3 (cont.)

Each of these four computations can be sent to a different processor if our computer has several CPUs. By the above calculation, we know that $2134 \cdot 1531$ is a solution of the system

$$x \equiv 9 \pmod{95}$$
$$x \equiv 0 \pmod{97}$$
$$x \equiv 30 \pmod{98}$$
$$x \equiv 55 \pmod{99}$$

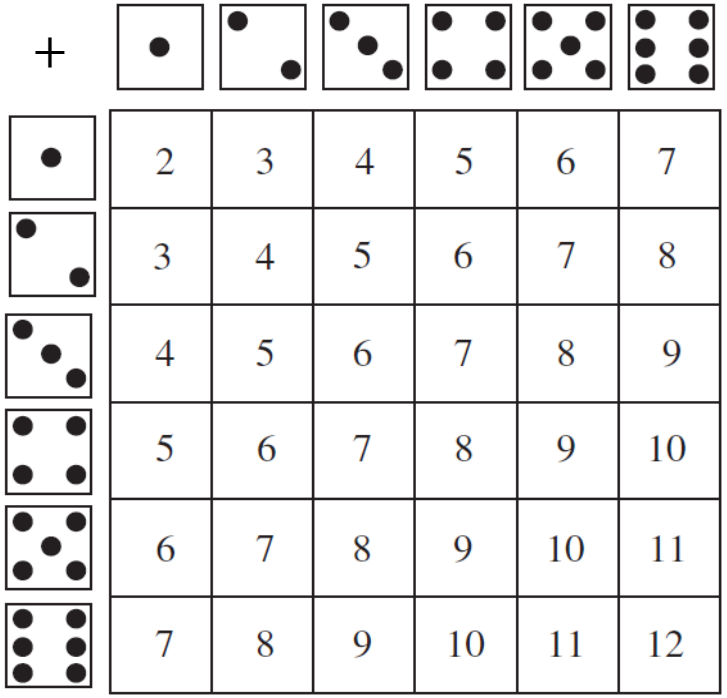
The Chinese Remainder Theorem tells us that solutions are unique up to modulo $95 \cdot 97 \cdot 98 \cdot 99 = 89{,}403{,}930$. Solving this system of congruences for x tells us that $2134 \cdot 1531 = 3{,}267{,}154$.

The conversion of the computation into the **four subcomputations** will take some computing time. In addition, solving the system of congruences can also take considerable time. However, if we have many computations to be performed on a particular set of numbers, it makes sense to transform the problem as we have done above and to perform the necessary calculations simultaneously.

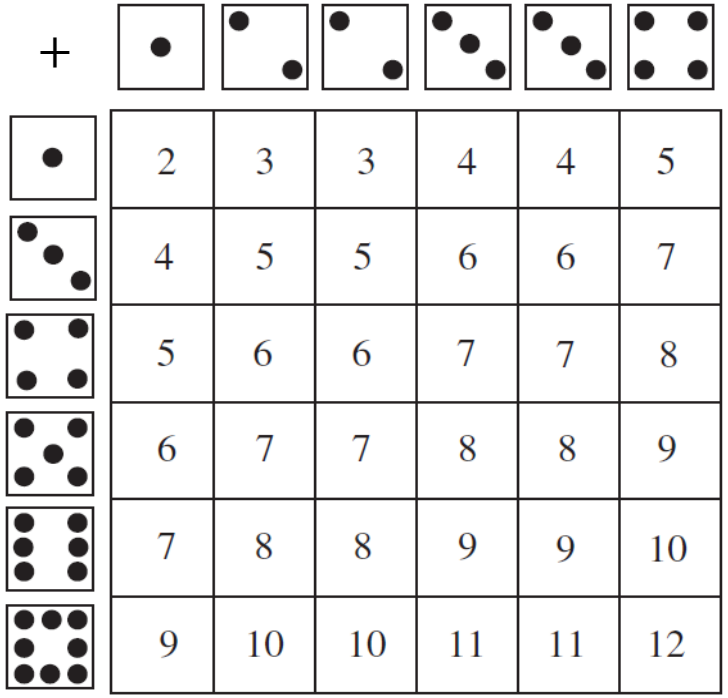
*13.2 Weird Dice (サイコロ): An Application of Unique Factorization

*13.2 Weird Dice (サイコロ): An Application of Unique Factorization

Consider **an ordinary pair of dice whose faces are labeled 1 through 6. The probability of rolling a sum of 2 is 1/36, the probability of rolling a sum of 3 is 2/36, and so on.**
In a 1978 issue of Scientific American [1], Martin Gardner remarked that if one were to label the six faces of one cube with the integers 1, 2, 2, 3, 3, 4 and the six faces of another cube with the integers 1, 3, 4, 5, 6, 8, then **the probability of obtaining any particular sum with these dice (called Sicherman dice)** would be **the same as the probability of rolling that sum with ordinary dice** (that is, 1/36 for a 2, 2/36 for a 3, and so on). See Figure 13.1.



+						
	2	3	4	5	6	7
	3	4	5	6	7	8
	4	5	6	7	8	9
	5	6	7	8	9	10
	6	7	8	9	10	11
	7	8	9	10	11	12



+						
	2	3	3	4	4	5
	4	5	5	6	6	7
	5	6	6	7	7	8
	6	7	7	8	8	9
	7	8	8	9	9	10
	9	10	10	11	11	12

Figure 13.1

*13.2 Weird Dice (サイコロ): An Application of Unique Factorization

In this subsection, **we show how the Sicherman labels can be derived**, and that they are the only possible such labels besides 1 through 6. **To do so, we utilize the fact that $\mathbb{Z}[x]$ has the unique factorization property**.

To begin, let us ask **ourselves how we may obtain a sum of** 6, say, **with an ordinary pair of dice**. Well, **there are five possibilities for the two faces** (5, 1), (4, 2), (3, 3), (2, 4), and (1, 5). Next we consider the product of the two polynomials created by using the ordinary dice labels as exponents:

$$(x^6 + x^5 + x^4 + x^3 + x^2 + x)(x^6 + x^5 + x^4 + x^3 + x^2 + x)$$

Observe that we pick up the term x^6 in this product in precisely the following ways: $x^5 \cdot x^1$, $x^4 \cdot x^2$, $x^3 \cdot x^3$, $x^2 \cdot x^4$, $\mathrm{x}^1 \cdot x^5$. Notice the correspondence between pairs of labels whose sums are 6 and pairs of terms whose products are x^6.

*13.2 Weird Dice (サイコロ): An Application of Unique Factorization

This correspondence is ***one-to-one***, and it is valid for all sums and all dice—including the Sicherman dice and any other dice that yield the desired probabilities. So, let $a_1, a_2, a_3, a_4, a_5, a_6$ and $b_1, b_2, b_3, b_4, b_5, b_6$ be any two lists of positive integer labels for the faces of a pair of cubes with the property that the probability of rolling any particular sum with these dice (let us call them weird dice) is the same as the probability of rolling that sum with ordinary dice labeled 1 through 6. Using our observation about products of polynomials, this means that

$$(x^6 + x^5 + x^4 + x^3 + x^2 + x)(x^6 + x^5 + x^4 + x^3 + x^2 + x)$$

$$= (x^{a_1} + x^{a_2} + x^{a_3} + x^{a_4} + x^{a_5} + x^{a_6})(x^{b_1} + x^{b_2} + x^{b_3} + x^{b_4} + x^{b_5} + x^{b_6})$$

Now all we have to do is solve this equation for the a's and b's. Here is where unique factorization in $\mathbb{Z}[x]$ comes in.

*13.2 Weird Dice (サイコロ): An Application of Unique Factorization

The polynomial $x^6 + x^5 + x^4 + x^3 + x^2 + x$ factors uniquely into irreducibles as

$$x(x+1)(x^2+x+1)(x^2-x+1)$$

so that the left-hand side of Equation 13.1 has the irreducible factorization

$$x^2(x+1)^2(x^2+x+1)^2(x^2-x+1)^2$$

So, by Theorem 13.2 (see page 20), this means that these factors are the only possible irreducible factors of $P(x) = x^{a_1} + x^{a_2} + x^{a_3} + x^{a_4} + x^{a_5} + x^{a_6}$. Thus, $P(x)$ has the form

$$x^q(x+1)^r(x^2+x+1)^t(x^2-x+1)^u$$

where $0 \leq q, r, t, u \leq 2$.

*13.2 Weird Dice (サイコロ): An Application of Unique Factorization

To restrict further the possibilities for these four parameters, we evaluate $P(1)$ in two ways. $P(1) = 1^{a_1} + 1^{a_2} + 1^{a_3} + 1^{a_4} + 1^{a_5} + 1^{a_6} = 6$ and $P(1) = 1^q 2^r 3^t 1^u$. Clearly, this means that $r = 1$ and $t = 1$. What about q? Evaluating $P(0)$ in two ways shows that $q \neq 0$. On the other hand, if $q = 2$, the smallest possible sum one could roll with the corresponding labels for dice would be 3. Since this violates our assumption that smallest sum is 2, we have now reduced our list of possibilities for q, r, t, and u to $q = 1, r = 1, t = 1$, and $u = 0, 1, 2$. Let's consider each of these possibilities in turn.

When $u = 0$, $P(x) = x^4 + x^3 + x^3 + x^2 + x^2 + x$, so the die labels are $4, 3, 3, 2, 2, 1$—a Sicherman die.

When $u = 1$, $P(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x$, so the die labels are $6, 5, 4, 3, 2, 1$—an ordinary die.

When $u = 2$, $P(x) = x^8 + x^6 + x^5 + x^4 + x^3 + x$, so the die labels are $8, 6, 5, 4, 3, 1$—the other Sicherman die.

This proves that the Sicherman dice do give the same probabilities as ordinary dice *and* that they are the ***only*** other pair of dice that have this property.

Theorem 13.2 (Unique Factorization in $\mathbb{Z}[x]$)

Every polynomial in $\mathbb{Z}[x]$ that is not the zero polynomial or a unit in $\mathbb{Z}[x]$ can be written in the form $a_1 a_2 \cdots a_s \, p_1(x) p_2(x) \cdots p_m(x)$, where the a_i's are irreducible polynomials of degree 0 and the $p_i(x)$'s are irreducible polynomials of positive degree. Furthermore, if

$$a_1 a_2 \cdots a_s \, p_1(x) p_2(x) \cdots p_m(x) = b_1 b_2 \cdots b_t q_1(x) q_2(x) \cdots q_n(x)$$

where the a_i's and b_i's are irreducible polynomials of degree 0 and the $p_i(x)$'s and $q_i(x)$'s are irreducible polynomials of positive degree, then $s = t$, $m = n$, and, after renumbering the b's and $q(x)$'s, we have $a_i = \pm b_i$ for $i = 1, \ldots, s$ and $p_i(x) = \pm q_i(x)$ for $i = 1, \ldots, m$.

Review for Lecture 13

- The Chinese Remainder Theorem (中国の剰余定理)
- Simultaneous Congruences
- Unique Factorization in $\mathbb{Z}[x]$

Assignment

No assignment for this lecture.

(It suggests to read Chapter 8 Algebraic Coding Theory of the textbook.)

References

[1] Thomas W. Judson etc. Abstract Algebra Theory and Applications, 2018
[2] D. S. Malik, John N. Mordeson, M.K. Sen, Introduction to Abstract Algebra, 2007
[3] **(おすすめ)** 松本 眞, 代数系への入門, http://www.math.sci.hiroshima-u.ac.jp/~m-mat/TEACH/daisu-nyumon2014.pdf
[4] Wikipedia
[5] Materials from internet.