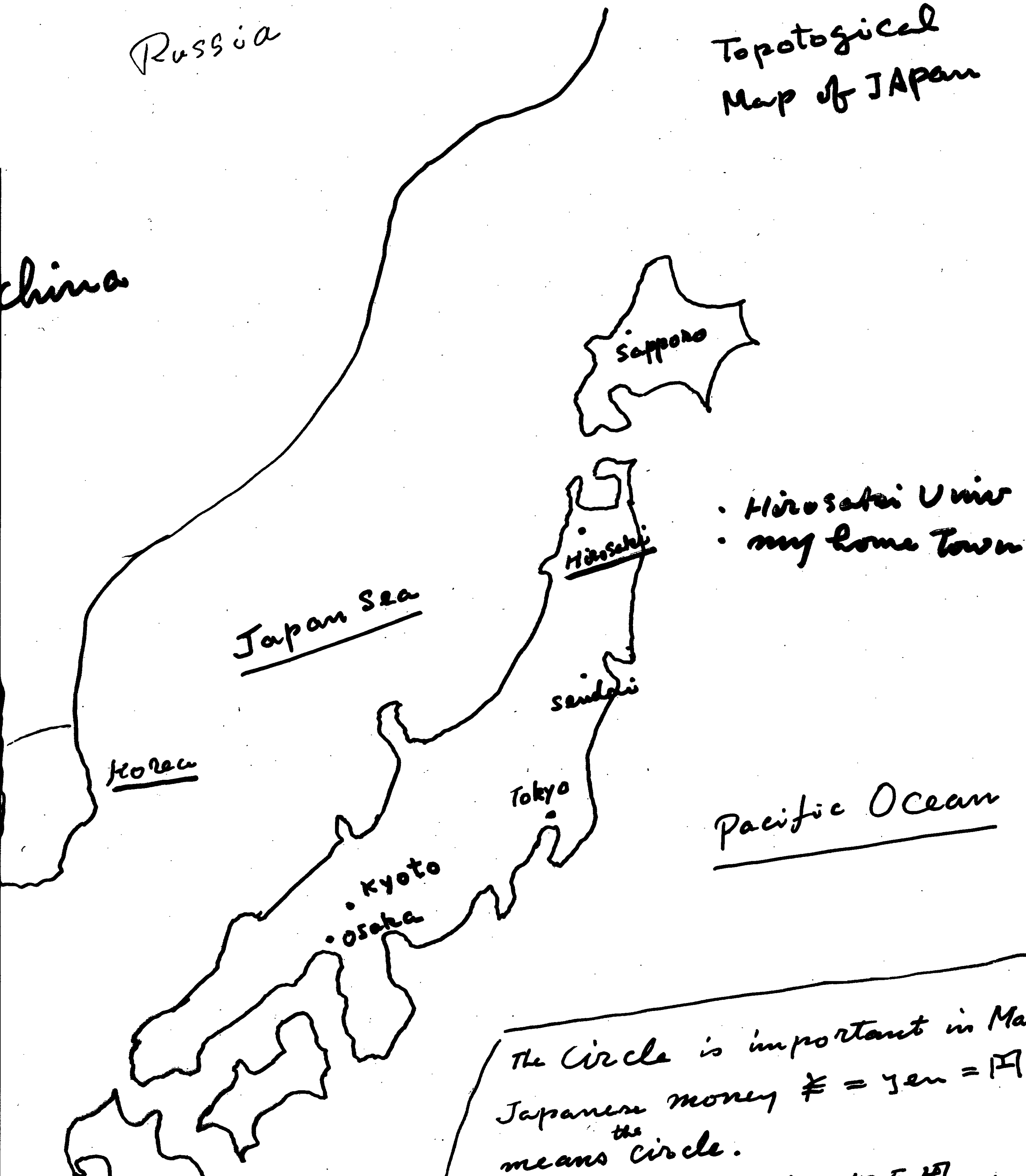
On cyclotomic polynomials

K. Motose

Copernics Univ., Torun, Poland での講演 (Nov. 1, 2002) の OHP 原稿。

June 2003 本瀬香

Location of Hirosaki



The Circle is important in Math

Japanese money ¥ = Yen = 円 means the circle.

my Travel fee is 12万円 = 120000 Yen

万 = ten thousant

1円 = Yen

On ~~values of~~ cyclotomic polynomials

K. Motose

November 5th 2002

1. Definitions

Cyclotomic polynomials are defined by

$$\underline{\Phi_n(x) = \prod_{(k,n)=1} (x - \zeta_n^k)}$$

$\varphi(n) = \deg \Phi_n(x)$

where $\zeta_n = \cos\left(\frac{2\pi}{n}\right) + \sqrt{-1}\sin\left(\frac{2\pi}{n}\right)$ and the product is extended over natural numbers k which are relatively prime to n with $1 \le k \le n$.

Example.

$$\Phi_1(x) = x - 1,\ \Phi_2(x) = x + 1,\ \Phi_3(x) = x^2 + x + 1,$$
$$\Phi_4(x) = x^2 + 1,\ \Phi_5(x) = x^4 + x^3 + x^2 + x + 1,$$
$$\Phi_6(x) = x^2 - x + 1,\ \ldots$$

Möbius' function μ is also defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } p^2 \mid n \text{ for a prime } p, \\ (-1)^r & \text{if } n = p_1p_2\ldots p_r \text{ where } p_k \text{ are all} \\ & \text{distinct primes.} \end{cases}$$

Example.

$$\mu(1) = 1,\ \mu(2) = -1,\ \mu(3) = -1,\ \mu(4) = 0,$$
$$\mu(5) = -1, \mu(6) = 1,\ \ldots$$

Fundamental properties

We can now state fundamental properties of cyclotomic polynomials.

1. $x^n - 1 = \prod_{d|n} \Phi_d(x)$ where d runs through positive divisors of n. Thus $n = \sum_{d|n} \varphi(d)$.
2. $\Phi_n(x) \in \boldsymbol{Z}[x]$ and the leading coefficient of $\Phi_n(x)$ is 1.
3. $\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(\frac{n}{d})}$. Thus $\varphi(n) = \sum_{d|n} d\mu(\frac{n}{d})$.
4. $\Phi_n(x)$ is irreducible in $\boldsymbol{Q}[x]$.

1. This formula is equivalent to the definition of cyclotomic polynomials.
2. It is easy to see from the above that $\Phi_n(a)$ is an integer for an integer a. It is important for us.
3. This formula is useful for calculations of cyclotomic polynomials. For example,

$$\Phi_6(x) = \frac{(x^6-1)(x-1)}{(x^3-1)(x^2-1)} = \frac{x^3+1}{x+1} = x^2 - x + 1$$

4. This is essential for Gauss' theorem which give necessary and sufficient condition that regular polygon can be constructed by using only ruler and compass. Galois groups of cyclotomic fields are determined from this.

We provide an estimation of values of cyclotomic polynomials.

Theorem 1. $\Phi_n(x)$ are strictly increasing functions for $x \geq 2$ and

$$a^{\varphi(n)+1} > \Phi_n(a) > a^{\varphi(n)-1} \quad \text{for } n, a \geq 2.$$

where $\varphi(n)$ is the degree of $\Phi_n(x)$ which is the number of positive integers $k < n$ with $(k, n) = 1$.

Example. $\Phi_6(x) = x^2 - x + 1$ is strictly increasing for $x \geq 1$ and $a^3 > a^2 - a + 1 > a$ for $a \geq 2$.

Fermat's little Theorem. If p is a prime and a is a positive integer with $p \not| a$, then $a^{p-1} \equiv 1 \bmod p$.

Example. $3^6 \equiv 1 \bmod 7$.

If p is a prime and a is a positive integer with $p \not| a$, then the least positive integer s such that $a^s \equiv 1 \bmod p$ is called the order of a modulo p. We denote the order of a modulo p by $|a|_p$. It is easy to show that $|a|_p$ is a divisor of m if $a^m \equiv 1 \bmod p$.

Example. We have $|2|_7 = 3$ from

$$2^1 \equiv 2 \bmod 7,\ \ 2^2 \equiv 4 \bmod 7,\ \ 2^3 \equiv 1 \bmod 7$$

Let q be a prime divisor of a Mersenne number $2^p - 1$ where p is prime. Then $p = |2|_q$ since p is prime. Thus p is a divisor of $q-1$ and $q > p$. This shows that there exist infinitely many prime numbers. In fact, starting from 2 we have $3,\ 7,\ 127, \ldots$. In this argument, $p = |2|_q$ is most important. We can generalized this to the next theorem which is easy to prove, but powerful for us.

Theorem 2. If $p \mid \Phi_n(a)$, then $n = p^e|a|_p$.

Example. Since $\Phi_{18}(2) = 3{\cdot}19$, we have $18 = 3^2{\cdot}|2|_3 = |2|_{19}$. For the numbers 18 and 2, we can find a prime 19 with $18 = |2|_{19}$. But for number 6 and 2, we cannot find such a prime because $\Phi_6(2) = 3$. This is the only exceptional case in the next theorem.

The next was known before one century more and was found again by many mathematicians, but is not so popular for us. This follows from the above theorem and an estimation cited before.

Theorem 3 (Bang). If $n \geq 3, a \geq 2$ and $(n, a) \neq (6, 2)$, then there exists a prime p with $n = |a|_p$.

4. Applications to algebra

Cyclotomic polynomials provide some important theorems on algebra.

1. The multiplicative group of a finite field is cyclic.
2. Artin's theorem with respect to the orders of finite (linear) simple groups.
3. Wedderburn's theorem: Finite division rings are commutative.
4. Special case of Dirichlet's theorem: The next arithmetic progression for a natural number d contains infinitely many primes.

   $$1,\ 1+d,\ 1+2d,\ \dots,\ 1+nd,\ \dots .$$

5. There exists a Galois extension over the rational number field such that a given finite abelian group is the Galois group of this extension.
6. Primality tests of big primes.

1. It is easy to prove from Theorem 2 and the next equation for a prime field F_p

   $$\prod_{d|p-1} \Phi_d(x) = x^{p-1} - 1 = \prod_{\alpha \in F_p^*} (x - \alpha).$$

   Just a modification of Theorem 2 gives the same proof in general.

2. For example, we set the next number $N_n(q)$ for a natural number $n \geq 2$ and a prime power $q = p^r$ where p is prime. This number is the order of the projective special linear group $\mathrm{PSL}(n, q)$

$$N_n(q) = \frac{1}{(n, q-1)} q^{\frac{n(n-1)}{2}} (q^n - 1)(q^{n-1} - 1) \cdots (q^2 - 1)$$

If $N_n(q) = N_{n_0}(q_0)$ for different pairs $(n, q) \neq (n_0, q_0)$, then $N_3(4) = N_4(2) = 20160, N_2(7) = N_3(2) = 168$, and $N_2(5) = N_2(4) = 60$.

3. In the last part of Witt's proof, we have the equation $\Phi_n(q)|q-1$. This contradicts to $\Phi_n(q) > q-1$. However, [illegible] $n>1$ It is easy to see $n = 1$ from Theorem 2.

4. It is a special case but is used frequently.

5. No comments.

6. For example, the next is an extension of Lucas' or Pepin's test.

Theorem 4. (1) $p > 3$ is prime if and only if there exists an integer c such that $\left(\frac{c}{p}\right) = -1$ and $\Phi_{p-1}(c) \equiv 0 \bmod p$.

(2) $p > 3$ is prime if and only if there exists an integer $c > 1$ such that $(c^3 - c, p) = 1, \gamma = c + \sqrt{c^2 - 1}$, $\left(\frac{2c+2}{p}\right) = \left(\frac{c^2-1}{p}\right) = -1$ and $\Phi_{p+1}(\gamma) \equiv 0 \bmod p\mathcal{O}_\gamma$ where $\mathcal{O}_\gamma$ is the ring of algebraic integers in $\boldsymbol{Q}(\gamma)$

5. Cipher

Pseudo primes are useful for a cipher.

Definition. A composite number n is a a-pseudo prime if and only if $a^{n-1} \equiv 1 \bmod n$

Roughly speaking, every a-pseudo primes is a product of divisors of cyclotomic numbers $\Phi_n(a)'s$ for some n, and conversely. The next is a special case, but useful for a cipher.

Theorem 5. If d is a divisor of $\Phi_n(a)$ and $(d, n) = 1$, then $\underline{a^{d-1} \equiv 1 \bmod\ d}$

We shall present a cipher using cyclotomic polynomials. We shall represent by $\boldsymbol{Z}^s$ the direct sum of the ring $\boldsymbol{Z}$ of integers. Let $\mathbf{1}, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{n}$ be the elements of $\boldsymbol{Z}^s$ such that $\mathbf{1} = (1, 1, \ldots, 1)$ is the identity of $\boldsymbol{Z}^n$,

$$\boldsymbol{a} = (a_1, a_2, \ldots, a_s), \boldsymbol{b} = (b_1, b_2, \ldots, b_s), \text{ and}$$
$$\boldsymbol{n} = (n_1, n_2, \ldots, n_s)$$

We use the following notations.

$\boldsymbol{a} \equiv \boldsymbol{b} \bmod \boldsymbol{n}$ if and only if $a_k \equiv b_k \bmod n_k$ for every k.
$(\boldsymbol{a}, \boldsymbol{b}) = \mathbf{1}$ if and only if $(a_k, b_k) = 1$ for every k.
$\boldsymbol{a}^{\boldsymbol{n}} = (a_1^{n_1}, a_2^{n_2}, \ldots, a_s^{n_s})$.

We can construct a cipher as follows: For a plain text $\boldsymbol{a}$, let $\boldsymbol{k} = (k_1, k_2, \ldots, k_s)$ and $\boldsymbol{\ell} = (\ell_1, \ell_2, \ldots, \ell_s)$ be vectors such that k_i and ℓ_i are divisors of $\Phi_{s_i}(a_i)$ with $(k_i, s_i) = 1$ and $\Phi_{t_i}(a_i)$ with $(\ell_i, t_i) = 1$ where $(s_i, t_i) = 1$, respectively. We set $\boldsymbol{n} = \boldsymbol{k\ell}$ and $\boldsymbol{m} = (\boldsymbol{k} - 1)(\boldsymbol{\ell} - 1)$. Then we can see

$$\underline{\boldsymbol{a}^{\boldsymbol{m}} \equiv 1 \bmod \boldsymbol{n}.}$$

We choose an enciphering key e with $(e, \boldsymbol{m}) = 1$ and calculate the deciphering key d with $\underline{ed \equiv 1 \bmod \boldsymbol{m}}$. Then the sender A encipher $\boldsymbol{a}$ with $\boldsymbol{b} \equiv \boldsymbol{a}^{e} \bmod \boldsymbol{n}$ and A sends $\boldsymbol{b}$ to the receiver B. Then B decipher $\boldsymbol{b}$ using relationship

$$\boldsymbol{b}^{d} \equiv \boldsymbol{a}^{ed} \equiv \boldsymbol{a} \bmod \boldsymbol{n}.$$

Example To encipher a word "BULLETIN", we first translate "BULLETIN" into this numerical equivalence $\boldsymbol{a} = (2,3,4,4,5,6,7,8)$. We choose the next vectors $\boldsymbol{k}, \boldsymbol{\ell}$ for $\boldsymbol{a}$.

$$\begin{aligned}
\boldsymbol{k} &= (\Phi_5(2), \Phi_5(3), \Phi_5(4), \Phi_5(4), \Phi_5(5), \tfrac{1}{5}\Phi_5(6), \\
&\quad \Phi_5(7), \Phi_5(8)) \\
\boldsymbol{\ell} &= (\Phi_9(2), \Phi_9(3), \tfrac{1}{3}\Phi_9(4), \tfrac{1}{3}\Phi_9(4), \Phi_9(5), \Phi_9(6), \\
&\quad \tfrac{1}{3}\Phi_9(7), \Phi_9(8))
\end{aligned}$$

Then we set

$$\boldsymbol{n} = \boldsymbol{k\ell},\ \boldsymbol{m} = (\boldsymbol{k} - 1)(\boldsymbol{\ell} - 1)$$

Selecting the enciphering key $\boldsymbol{e} = 291$ with $(\boldsymbol{m}, \boldsymbol{e}) = 1$, we calculate the deciphering key

$$\begin{aligned}
\boldsymbol{d} &= (149, 56309, 48749, 48749, 5507069, 13528229, \\
&\quad 60758069, 296710709)
\end{aligned}$$

such that $\boldsymbol{ed} \equiv 1 \bmod \boldsymbol{m}$. After this setting, we use the following sequences of steps.

$$\begin{aligned}
\boldsymbol{\alpha} &= (B, U, L, L, E, T, I, N) \\
\boldsymbol{a} &= (2, 3, 4, 4, 5, 6, 7, 8) \\
\boldsymbol{b} &\equiv \boldsymbol{a}^{\boldsymbol{e}} \bmod \boldsymbol{n} \\
&= (1318, 72681, 302382, 302382, 11340745, \\
&\quad 10593334, 96832971, 1191412216) \\
\boldsymbol{b}^{\boldsymbol{d}} \bmod \boldsymbol{n} &= (2, 3, 4, 4, 5, 6, 7, 8) \\
\boldsymbol{\alpha} &= (B, U, L, L, E, T, I, N)
\end{aligned}$$

Problem

Factorize $\Phi_{97}(10) = \dfrac{10^{97}-1}{10-1} = \overbrace{111\cdots1}^{97}$

Golay Code

$\Phi_n(x) \bmod p \;=\; f_1(x)\cdots f_r(x)$

$f_k(x)$ has same degree $|p|_n$ $\qquad |2|_{23} = 11$

the order of $p \bmod n$

$$\underset{x^{22}+\cdots+x+1}{\Phi_{\underset{11}{23}}(x)} \bmod 2 = \underline{(x^{11}+x^9+x^7+x^6+x^5+x+1)} \cdot (x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)$$

generator poly of Golay code $\qquad$ min-distance $= 7$

= one of two factors of $\Phi_{23}(x)$

Factorization of numbers

$1 < n \in \mathbb{N}$, Find $a, m \in \mathbb{N}$ s.t. $(am, n) = 1$ and $a^m \equiv 1\ (n)$. Then we have –

$$\boxed{n = \prod_{d \mid m} (n, \Phi_d(a))}$$