Bounds on Cyclotomic Numbers

Do Duc Tai
Nanyang Technological University, Singapore
(joint with B. Schmidt, K. H. Leung)

Kloster Irsee, 15 September 2017

Cyclotomic Numbers

- q a prime power: $q = p^n = ef + 1$.
- g primitive in $\mathbb{F}_q$, $\mathbb{F}_q^* = \{1, g, \dots, g^{ef-1}\}$. For $a \in \mathbb{N}$,

$$C_a = \left\{g^a, g^{a+e}, \dots, g^{a+(f-1)e}\right\} = g^a C_0.$$

- $a, b \in \mathbb{N}$, (a, b) a cyclotomic number of order e:

$$(a, b) = \#\, solutions\ 1 + x = y, x \in C_a, y \in C_b,$$

$$(a, b) = \#\, pairs\ (r, s): 0 \le r, s \le f - 1, 1 + g^{a+re} = g^{b+se}.$$

Uniformity of Cyclotomic Numbers

$$(a,b) = \#\, solutions\ 1 + x = y, x \in C_a, y \in C_b.$$

- $\mathbb{F}_q^* = \cup_{a=0}^{e-1} C_a$. If $y \neq 1$, then $1 - y \in C_a$ for some $0 \leq a \leq e-1$:

$$\sum_{a=0}^{e-1}(a,b) = f - \delta_{b0} \approx q/e.$$

  Fixing e and let $q \gg e$, then $(a,b) = q/e^2 + O(\sqrt{q})$ (Katre 1989).

- Fixing f and let $q \gg f$, how are the values of (a,b)?

  Answer: they are "*uniformly small*".

Results by Betsumiya et al., 2013

a) $(a, b) \leq \left\lfloor \frac{f}{2} \right\rfloor$ if $p > \frac{3f}{2} - 1.$

b) $(0,0) = 0$ if $f \not\equiv 0 \bmod 6$ and $p \gg f$.

c) $(0,0) = 2$ if $f \equiv 0 \bmod 6$ and $p \gg f$.

How “large” exactly does p need to be compared to f?

Results by Betsumiya et al., 2013

$$M = \begin{pmatrix} 1 & \binom{f}{1} & \cdots & \binom{f}{f-2} & \binom{f}{f-1} \\ \binom{f}{f-1} & 1 & & \binom{f}{f-3} & \binom{f}{f-2} \\ \vdots & & \ddots & \vdots & \\ \binom{f}{2} & \binom{f}{3} & & 1 & \binom{f}{1} \\ \binom{f}{1} & \binom{f}{2} & \cdots & \binom{f}{f-1} & 1 \end{pmatrix}_{f\times f}.$$

- If $p > |\det(M)|$, then $(0,0) \in \{0,2\}$.
- (Hadamard's inequality) If $p > \left(2^f - 1\right)^f$, then $(0,0) \in \{0,2\}$.

Our Results

(General Result)

If

$$p > \left(\sqrt{14}\right)^{f/ord_f(p)},$$

then

$$(a, b) \leq 3.$$

Our approach

- **Lemma 1**: $h(x)=\sum_{i=0}^{f-1} a_i x^i \in \mathbb{Z}[x]$. If

$$p^{ord_f(p)} > \left(\frac{f}{\varphi(f)}\sum_{i=0}^{k-1} a_i^2\right)^{\varphi(f)/2},$$

then

$$h(g^e)=0 \text{ over } \mathbb{F}_q \Leftrightarrow h(\zeta_f)=0 \text{ over } \mathbb{C}.$$

- **Lemma 2 (Conway, Jones):** If S is a vanishing sum of roots of unity of length ≤ 6, then S contains subsums each of which is *similar* to

$$1+\zeta_2 \text{ or } 1+\zeta_3+\zeta_3^2 \text{ or}$$

$$1+\zeta_5+\zeta_5^2+\zeta_5^3+\zeta_5^4 \text{ or } -\zeta_3-\zeta_3^2+\zeta_5+\zeta_5^2+\zeta_5^3+\zeta_5^4.$$

Proof of Lemma 1

➢ **Lemma 1**: $p^{ord_f(p)} > \left(\frac{f}{\varphi(f)}\sum_{i=0}^{f-1} a_i^2\right)^{\varphi(f)/2}$, then

$$h(g^e) = 0 \text{ over } \mathbb{F}_q \Leftrightarrow h(\zeta_f) = 0 \text{ over } \mathbb{C}.$$

<u>Proof</u>

- **<u>Claim</u>**: We have

$$\left|N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}}\left(h(\zeta_f)\right)\right| \leq \left(\frac{f}{\varphi(f)}\sum_{i=0}^{f-1} a_i^2\right)^{\varphi(f)/2}.$$

- By Claim,

$$p^{ord_f(p)} > \left|N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}}\left(h(\zeta_f)\right)\right|.$$

Proof of Lemma 1

- $\wp$ a prime ideal of $\mathbb{Z}[\zeta_f]$ above p, $m = ord_f(p) \mid n$,

$$\mathbb{Z}[\zeta_f]/\wp \cong \mathbb{F}_{p^m} \leq \mathbb{F}_q = \mathbb{F}_{p^n}.$$

- Isomorphism $\phi: \mathbb{F}_{p^m} \to \mathbb{Z}[\zeta_f]/\wp$,

$\phi(g^e)$ a primitive f^{th} root of unity:

$$\phi(g^e) = \zeta_f^j + \wp, (j, f) = 1,$$

$$\phi(h(g^e)) = h\left(\zeta_f^j\right) + \wp,$$

$$h(g^e) = 0 \Leftrightarrow h\left(\zeta_f^j\right) \in \wp.$$

Proof of Lemma 1

$$h(g^e) = 0 \Leftrightarrow h\left(\zeta_f^j\right) \in \wp.$$

$(\Leftarrow)$ $h\left(\zeta_f\right) = 0 \to h\left(\zeta_f^j\right) = 0 \in \wp \to h(g^e) = 0.$

$(\Rightarrow)$ $h(g^e) = 0 \to h\left(\zeta_f^j\right) \in \wp \to N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}}\left(h\left(\zeta_f^j\right)\right) \equiv 0 \pmod{p^m}.$

If $h\left(\zeta_f\right) \neq 0$, then $h\left(\zeta_f^j\right) \neq 0$ and

$$\left|N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}}\left(h\left(\zeta_f^j\right)\right)\right| \geq p^m,$$

contradiction.

Application of Lemma 1

- $(0,0) = \#\,(r,s)$ with $0 \le r,s \le f-1$ and $1 + g^{re} = g^{se}$.
  $h(x) = 1 + x^r - x^s$, then $h(g^e) = 0$ and
  $$p^{ord_f(p)} > \left(\frac{3f}{\varphi(f)}\right)^{\varphi(f)/2} \rightarrow 1 + \zeta_f^r - \zeta_f^s = 0.$$
- **Theorem 1**: If
  $$p > \left(\frac{3f}{\varphi(f)}\right)^{\frac{\varphi(f)}{2ord_f(p)}},$$
  then
  $$(0,0) = \begin{cases} 0 \text{ if } f \not\equiv 0\ (mod\ 6) \text{ and } 2 \notin C_0, \\ 1 \text{ if } f \not\equiv 0\ (mod\ 6) \text{ and } 2 \in C_0, \\ 2 \text{ if } f \equiv 0\ (mod\ 6) \text{ and } 2 \notin C_0, \\ 3 \text{ if } f \equiv 0\ (mod\ 6) \text{ and } 2 \in C_0. \end{cases}$$

Discussion

- Can the bound between p and f be improved?

$$p > \left(\sqrt{14}\right)^{f/ord_f(p)} \Rightarrow (a,b) \leq 3.$$

Partial answer: ***Yes***

If f is a prime and if $p > 3^{f/ord_f(p)}$, then $(a,b) \leq 3$.

- Other numbers of similar types? For example

$$(a,b,c) = \#\, solutions\ 1 + x + y = z, x \in C_a, y \in C_b, z \in C_c.$$

Discussion

- Jacobi sums: $\mathbb{F}_q^* = \langle g \rangle,\ \chi \in \widehat{\mathbb{F}_q^*}\colon\ \chi(g) = \zeta_e.$

$$J(a,b) = \sum_{x \in \mathbb{F}_q} \chi^a(x)\chi^b(x+1)\,,$$

$$(a,b) = \frac{1}{e^2}\sum_{i,j} J(i,j)\zeta_e^{-(ai+bj)},$$

$$J(i,j) = \sum_{a,b} (a,b)\zeta_e^{ai+bj}\ .$$

Discussion

- Link to group ring equation:

Abelian $G = C_e \times C_e = \langle x\rangle \times \langle y\rangle$. Put

$$A = \sum_{i,j=0}^{e-1} (i,j)\, x^i y^j, X = \langle x\rangle, Y = \langle y\rangle, Z = \langle xy\rangle,$$

then

$$AA^{(-1)} = q - f(X + Y + Z) + f^2 G.$$

Thank You