On Consecutive Primitive nth Roots of Unity Modulo q

or

Finding Adjacent Elements of the Same Order in a Finite Field

Matthew Litman*
(Thomas Brazelton, Joshua Harrington, Siddarth Kannan)
Penn State University

MASON I
October 29th, 2016

Outline

Introduction and Inspiration

- For q prime, the field $\mathbb{Z}_q$ has a cyclic group of units $\mathbb{Z}_q^\times$.

Introduction and Inspiration

- For q prime, the field $\mathbb{Z}_q$ has a cyclic group of units $\mathbb{Z}_q^\times$.
- The subgroup structure of $\mathbb{Z}_q^\times$ has been well-studied.

Introduction and Inspiration

- For q prime, the field $\mathbb{Z}_q$ has a cyclic group of units $\mathbb{Z}_q^\times$.
- The subgroup structure of $\mathbb{Z}_q^\times$ has been well-studied.
- Little is known about the additive gaps between elements of the same multiplicative order.

Introduction and Inspiration

- For q prime, the field $\mathbb{Z}_q$ has a cyclic group of units $\mathbb{Z}_q^\times$.
- The subgroup structure of $\mathbb{Z}_q^\times$ has been well-studied.
- Little is known about the additive gaps between elements of the same multiplicative order.
- Here we aim to classify the positive integers n for which there exists a prime q so that $\mathbb{Z}_q$ contains adjacent elements of multiplicative order n.

Example: $\mathbb{Z}_{11}$

x	1	2	3	4	5	6	7	8	9	10
ord(x)	1	10	5	5	5	10	10	10	5	2

where the $ord(x)$ is the multiplicative order of x

Example: $\mathbb{Z}_{11}$

x	1	2	3	4	5	6	7	8	9	10
ord(x)	1	10	5	5	5	10	10	10	5	2

where the $ord(x)$ is the multiplicative order of x

Remark

Given n, we want to guarantee that modulo some prime q, we can find adjacent elements of order n.

Lucas Numbers and Mersenne Numbers

Definition

The nth Lucas number L_n is given by the linear recurrence

$$L_n = L_{n-1} + L_{n-2}$$

with the initial conditions $L_0 = 2$ and $L_1 = 1$.

Lucas Numbers and Mersenne Numbers

Definition

The nth Lucas number L_n is given by the linear recurrence

$$L_n = L_{n-1} + L_{n-2}$$

with the initial conditions $L_0 = 2$ and $L_1 = 1$.

Definition

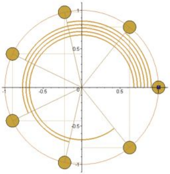
The nth Mersenne number is of the form $M_n = 2^n - 1$.

Outline

Cyclotomic Polynomials

Definition

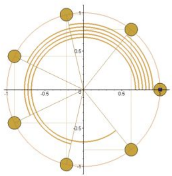
The nth cyclotomic polynomial, denoted $\Phi_n(x)$ is a monic, irreducible polynomial in $\mathbb{Z}[x]$ having the primitive nth roots of unity in the complex plane as its roots.



Cyclotomic Polynomials

Definition

The nth cyclotomic polynomial, denoted $\Phi_n(x)$ is a monic, irreducible polynomial in $\mathbb{Z}[x]$ having the primitive nth roots of unity in the complex plane as its roots.



- We may express this as

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

The Resultant

Definition

The resultant of two polynomials over a field K is defined as the product of the differences of their roots in the algebraic closure of K:

$$\mathrm{Res}(f,g) = \prod_{x,y\in\overline{K}:f(x)=g(y)=0}(x-y).$$

The Resultant

Definition

The resultant of two polynomials over a field K is defined as the product of the differences of their roots in the algebraic closure of K:

$$\mathrm{Res}(f,g) = \prod_{x,y\in\overline{K}:f(x)=g(y)=0}(x-y).$$

Remark

$\mathrm{Res}(f,g) \equiv 0 \pmod{q}$ *if and only if f and g share a root in* $\overline{\mathbb{Z}}_q$

Algebraic Integers and Norm

- An algebraic integer is a complex number that is the root of a polynomial with integer coefficients.

Algebraic Integers and Norm

- An algebraic integer is a complex number that is the root of a polynomial with integer coefficients.
- The field norm is a map that arises from certain types of field extensions.

Algebraic Integers and Norm

- An algebraic integer is a complex number that is the root of a polynomial with integer coefficients.
- The field norm is a map that arises from certain types of field extensions.
- The field norm of an algebraic integer is a rational integer.

Algebraic Integers and Norm

- An algebraic integer is a complex number that is the root of a polynomial with integer coefficients.
- The field norm is a map that arises from certain types of field extensions.
- The field norm of an algebraic integer is a rational integer.

Remark

We are concerned with the specific norm

$$N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n - \zeta_n^j + 1) := \prod_{\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})} \sigma(\zeta_n - \zeta_n^j + 1)$$
$$= \prod_{(i,n)=1} \zeta_n^i - \zeta_n^{ij} + 1$$

Boiling Down The Problem

- For prime $q > n$, an element $\alpha \in \mathbb{Z}_q$ has order n if and only if α is a root of $\Phi_n(x)$ in $\mathbb{Z}_q$.

Boiling Down The Problem

- For prime $q > n$, an element $\alpha \in \mathbb{Z}_q$ has order n if and only if α is a root of $\Phi_n(x)$ in $\mathbb{Z}_q$.
- So, α and $\alpha + 1$ are both of order n if and only if α is simultaneously a root of $\Phi_n(x)$ and $\Phi_n(x+1)$.

Boiling Down The Problem

- For prime $q > n$, an element $\alpha \in \mathbb{Z}_q$ has order n if and only if α is a root of $\Phi_n(x)$ in $\mathbb{Z}_q$.
- So, α and $\alpha + 1$ are both of order n if and only if α is simultaneously a root of $\Phi_n(x)$ and $\Phi_n(x+1)$.
- $\Phi_n(x)$ and $\Phi_n(x+1)$ will share some irreducible factor modulo q whenever $\mathrm{Res}(\Phi_n(x), \Phi_n(x+1)) \equiv 0 \pmod{q}$.

Boiling Down The Problem

- For prime $q > n$, an element $\alpha \in \mathbb{Z}_q$ has order n if and only if α is a root of $\Phi_n(x)$ in $\mathbb{Z}_q$.
- So, α and $\alpha + 1$ are both of order n if and only if α is simultaneously a root of $\Phi_n(x)$ and $\Phi_n(x+1)$.
- $\Phi_n(x)$ and $\Phi_n(x+1)$ will share some irreducible factor modulo q whenever $\mathrm{Res}(\Phi_n(x), \Phi_n(x+1)) \equiv 0 \pmod{q}$.
- It is also known that $\Phi_n(x)$ will split into linear factors mod q whenever $q \equiv 1 \pmod{n}$.

Boiling Down The Problem

- For prime $q > n$, an element $\alpha \in \mathbb{Z}_q$ has order n if and only if α is a root of $\Phi_n(x)$ in $\mathbb{Z}_q$.
- So, α and $\alpha + 1$ are both of order n if and only if α is simultaneously a root of $\Phi_n(x)$ and $\Phi_n(x+1)$.
- $\Phi_n(x)$ and $\Phi_n(x+1)$ will share some irreducible factor modulo q whenever $\mathrm{Res}(\Phi_n(x), \Phi_n(x+1)) \equiv 0 \pmod{q}$.
- It is also known that $\Phi_n(x)$ will split into linear factors mod q whenever $q \equiv 1 \pmod{n}$.
- We conclude that if we find a prime $q \equiv 1 \pmod{n}$ that divides $\mathrm{Res}(\Phi_n(x), \Phi_n(x+1))$, there are consecutive elements of order n modulo q.

Boiling Down The Problem, cont.

- For the remainder of this talk, we will refer to $\mathrm{Res}(\Phi_n(x), \Phi_n(x+1))$ as Γ_n.

Boiling Down The Problem, cont.

- For the remainder of this talk, we will refer to $\mathrm{Res}(\Phi_n(x), \Phi_n(x+1))$ as Γ_n.
- We have

$$\Gamma_n = \mathrm{Res}(\Phi_n(x), \Phi_n(x+1)) = \prod_{(i,n)=1} \prod_{(j,n)=1} (\zeta_n^i - \zeta_n^j + 1)$$
$$= \prod_{(i,n)=1} N(\zeta_n - \zeta_n^i + 1).$$

Boiling Down The Problem, cont.

- For the remainder of this talk, we will refer to $\mathrm{Res}(\Phi_n(x), \Phi_n(x+1))$ as Γ_n.
- We have

$$\Gamma_n = \mathrm{Res}(\Phi_n(x), \Phi_n(x+1)) = \prod_{(i,n)=1} \prod_{(j,n)=1} (\zeta_n^i - \zeta_n^j + 1)$$
$$= \prod_{(i,n)=1} N(\zeta_n - \zeta_n^i + 1).$$

- We are thus concerned with finding prime divisors of these norms which are 1 modulo n.

Lemmas

Lemma

For each $n > 6$, L_n has a primitive, odd prime divisor p such that $p \equiv 1 \pmod{2n}$.

Lemmas

Lemma

For each $n > 6$, L_n has a primitive, odd prime divisor p such that $p \equiv 1 \pmod{2n}$.

Lemma (Konvalina)

For n odd, $L_n = \prod_{i=1}^{n}(\zeta_n^{2i} + \zeta_n^{i} - 1) = \prod_{d|n} N(\zeta_d - \zeta_d^{d-1} + 1)$.

Lemmas

Lemma

For each $n > 6$, L_n has a primitive, odd prime divisor p such that $p \equiv 1 \pmod{2n}$.

Lemma (Konvalina)

For n odd, $L_n = \prod_{i=1}^{n}(\zeta_n^{2i} + \zeta_n^{i} - 1) = \prod_{d|n} N(\zeta_d - \zeta_d^{d-1} + 1)$.

Lemma

For any $n > 6$, every primitive prime divisor p of M_n satisfies $p \equiv 1 \pmod{n}$

Proof

Lemma

For any $n > 6$, every primitive prime divisor p of M_n satisfies $p \equiv 1 \pmod{n}$

Proof

Lemma

For any $n > 6$, every primitive prime divisor p of M_n satisfies $p \equiv 1 \pmod{n}$

- Suppose p is a primitive prime divisor of $M_n = 2^n - 1$.

Proof

Lemma

For any $n > 6$, every primitive prime divisor p of M_n satisfies $p \equiv 1 \pmod{n}$

- Suppose p is a primitive prime divisor of $M_n = 2^n - 1$.
- We have $2^n \equiv 1 \pmod{p}$, so $\mathrm{ord}_p(2) \mid n$.

Proof

Lemma

For any $n > 6$, every primitive prime divisor p of M_n satisfies $p \equiv 1 \pmod{n}$

- Suppose p is a primitive prime divisor of $M_n = 2^n - 1$.
- We have $2^n \equiv 1 \pmod{p}$, so $\mathrm{ord}_p(2) \mid n$.
- If $\mathrm{ord}_p(2) = d < n$, then $p \mid 2^d - 1$, which is a contradiction.

Proof

Lemma

For any $n > 6$, every primitive prime divisor p of M_n satisfies $p \equiv 1 \pmod{n}$

- Suppose p is a primitive prime divisor of $M_n = 2^n - 1$.
- We have $2^n \equiv 1 \pmod{p}$, so $\mathrm{ord}_p(2) \mid n$.
- If $\mathrm{ord}_p(2) = d < n$, then $p \mid 2^d - 1$, which is a contradiction.
- We conclude that $\mathrm{ord}_p(2) = n$, so $n \mid |\mathbb{Z}_p^\times| = p - 1$, and $p \equiv 1 \pmod{n}$.

Outline

Results

Theorem

There exists a prime q such that $\mathbb{Z}_q$ contains consecutive primitive nth roots of unity if and only if $n \neq 1, 2, 3, 6$.

Note that this statement is equivalent to the following:

We prove this theorem for $n > 6$ in three cases:

Results

Theorem

There exists a prime q such that $\mathbb{Z}_q$ contains consecutive primitive nth roots of unity if and only if $n \neq 1, 2, 3, 6$.

Note that this statement is equivalent to the following:

Theorem

There exists a prime $q \equiv 1 \pmod{n}$ dividing Γ_n if and only if $n \neq 1, 2, 3, 6$.

We prove this theorem for $n > 6$ in three cases:

Results

Theorem

There exists a prime q such that $\mathbb{Z}_q$ contains consecutive primitive nth roots of unity if and only if $n \neq 1, 2, 3, 6$.

Note that this statement is equivalent to the following:

Theorem

There exists a prime $q \equiv 1 \pmod{n}$ dividing Γ_n if and only if $n \neq 1, 2, 3, 6$.

We prove this theorem for $n > 6$ in three cases:

- n is odd.

Results

Theorem

There exists a prime q such that $\mathbb{Z}_q$ contains consecutive primitive nth roots of unity if and only if $n \neq 1, 2, 3, 6$.

Note that this statement is equivalent to the following:

Theorem

There exists a prime $q \equiv 1 \pmod{n}$ dividing Γ_n if and only if $n \neq 1, 2, 3, 6$.

We prove this theorem for $n > 6$ in three cases:

- n is odd.
- $n = 2k$ where k is odd.

Results

Theorem

There exists a prime q such that $\mathbb{Z}_q$ contains consecutive primitive nth roots of unity if and only if $n \neq 1, 2, 3, 6$.

Note that this statement is equivalent to the following:

Theorem

There exists a prime $q \equiv 1 \pmod{n}$ dividing Γ_n if and only if $n \neq 1, 2, 3, 6$.

We prove this theorem for $n > 6$ in three cases:

- n is odd.
- $n = 2k$ where k is odd.
- $n \equiv 0 \pmod{4}$.

The Proof

- First we suppose n is odd. By a previous lemma, the nth Lucas number has a primitive prime divisor q, where $q \equiv 1 \pmod{2n}$.

The Proof

- First we suppose n is odd. By a previous lemma, the nth Lucas number has a primitive prime divisor q, where $q \equiv 1 \pmod{2n}$.
- Observe that $L_n = \prod_{i=1}^{n}(\zeta_n^{2i} + \zeta_n^{i} - 1) = \prod_{d|n} N(\zeta_d - \zeta_d^{d-1} + 1)$, and $N(\zeta_n - \zeta_n^{n-1} + 1) \mid \Gamma_n$.

The Proof

- First we suppose n is odd. By a previous lemma, the nth Lucas number has a primitive prime divisor q, where $q \equiv 1 \pmod{2n}$.
- Observe that $L_n = \prod_{i=1}^{n}(\zeta_n^{2i} + \zeta_n^{i} - 1) = \prod_{d|n} N(\zeta_d - \zeta_d^{d-1} + 1)$, and $N(\zeta_n - \zeta_n^{n-1} + 1) \mid \Gamma_n$.
- If $q \nmid N(\zeta_n - \zeta_n^{n-1} + 1)$, then $q | N(\zeta_d - \zeta_d^{d-1} + 1)$ for some $d < n$.

The Proof

- First we suppose n is odd. By a previous lemma, the nth Lucas number has a primitive prime divisor q, where $q \equiv 1 \pmod{2n}$.
- Observe that $L_n = \prod_{i=1}^{n}(\zeta_n^{2i} + \zeta_n^{i} - 1) = \prod_{d|n} N(\zeta_d - \zeta_d^{d-1} + 1)$, and $N(\zeta_n - \zeta_n^{n-1} + 1) \mid \Gamma_n$.
- If $q \nmid N(\zeta_n - \zeta_n^{n-1} + 1)$, then $q|N(\zeta_d - \zeta_d^{d-1} + 1)$ for some $d < n$.
- This implies that $q|L_d$, which is a contradiction!

The Proof

- First we suppose n is odd. By a previous lemma, the nth Lucas number has a primitive prime divisor q, where $q \equiv 1 \pmod{2n}$.
- Observe that $L_n = \prod_{i=1}^{n} (\zeta_n^{2i} + \zeta_n^{i} - 1) = \prod_{d|n} N(\zeta_d - \zeta_d^{d-1} + 1)$, and $N(\zeta_n - \zeta_n^{n-1} + 1) \mid \Gamma_n$.
- If $q \nmid N(\zeta_n - \zeta_n^{n-1} + 1)$, then $q | N(\zeta_d - \zeta_d^{d-1} + 1)$ for some $d < n$.
- This implies that $q | L_d$, which is a contradiction!
- We may conclude that $q \mid \Gamma_n$, so modulo q there are consecutive primitive nth roots of unity.

The Proof, cont.

The case where $n = 2k$, where k is odd, follows easily from the following fact.

Lemma

Whenever k is odd, $\Gamma_{2k} = \Gamma_k$.

The Proof, cont.

The case where $n = 2k$, where k is odd, follows easily from the following fact.

Lemma

Whenever k is odd, $\Gamma_{2k} = \Gamma_k$.

- We now treat the case where $4 \mid n$.

The Proof, cont.

- Suppose $4 \mid n$, and see that $N(\zeta_n - \zeta_n^{(n/2)+1} + 1) | \Gamma_n$.

The Proof, cont.

- Suppose $4 \mid n$, and see that $N(\zeta_n - \zeta_n^{(n/2)+1} + 1) | \Gamma_n$.
- Apply the observation that

$$\begin{aligned} N(\zeta_n - \zeta_n^{(n/2)+1} + 1) &= N(\zeta_n - (-1)\zeta_n + 1) = N(2\zeta_n + 1) \\ &= \prod_{(i,n)=1} (2\zeta_n^i + 1) = \prod_{(i,n)=1} -\zeta_n^i(-2 - \zeta_n^{-i}) \\ &= \prod_{(i,n)=1} (-2 - \zeta_n^{-i}) = \Phi_n(-2). \end{aligned}$$

The Proof, cont.

- Suppose $4 \mid n$, and see that $N(\zeta_n - \zeta_n^{(n/2)+1} + 1) | \Gamma_n$.
- Apply the observation that

$$\begin{aligned} N(\zeta_n - \zeta_n^{(n/2)+1} + 1) &= N(\zeta_n - (-1)\zeta_n + 1) = N(2\zeta_n + 1) \\ &= \prod_{(i,n)=1} (2\zeta_n^i + 1) = \prod_{(i,n)=1} -\zeta_n^i(-2 - \zeta_n^{-i}) \\ &= \prod_{(i,n)=1} (-2 - \zeta_n^{-i}) = \Phi_n(-2). \end{aligned}$$

- As $4 \mid n$, it can be shown that $\Phi_n(-2) = \Phi_n(2)$, which is the primitive part of the nth Mersenne number.

The Proof, cont.

- Suppose $4 \mid n$, and see that $N(\zeta_n - \zeta_n^{(n/2)+1} + 1) | \Gamma_n$.
- Apply the observation that

$$\begin{aligned} N(\zeta_n - \zeta_n^{(n/2)+1} + 1) &= N(\zeta_n - (-1)\zeta_n + 1) = N(2\zeta_n + 1) \\ &= \prod_{(i,n)=1} (2\zeta_n^i + 1) = \prod_{(i,n)=1} -\zeta_n^i(-2 - \zeta_n^{-i}) \\ &= \prod_{(i,n)=1} (-2 - \zeta_n^{-i}) = \Phi_n(-2). \end{aligned}$$

- As $4 \mid n$, it can be shown that $\Phi_n(-2) = \Phi_n(2)$, which is the primitive part of the nth Mersenne number.
- All primitive prime divisors q of the nth Mersenne number satisfy $q \equiv 1 \pmod{n}$, and the proof is complete.

The Exceptional Cases

The results on existence of primitive prime divisors for Lucas and Mersenne numbers holds for $n > 6$. We can easily calculate Γ_n for $n \leq 5$

$$\Gamma_1 = \Gamma_2 = 1$$

$$\Gamma_3 = \Gamma_6 = 4$$

$$\Gamma_4 = 5$$

$$\Gamma_5 = 121 = 11^2$$

When n is prime

For the case when $n = p$ is a prime number, we have an even easier time finding such a finite field.

Lemma

For a prime p, all primitive prime divisors of L_p are congruent to 1 modulo p.

Main Theorem and Some Interesting Corollaries

Theorem

There exists a prime q such that $\mathbb{Z}_q$ contains consecutive primitive nth roots of unity if and only if $n \neq 1, 2, 3, 6$.

Main Theorem and Some Interesting Corollaries

Theorem

There exists a prime q such that $\mathbb{Z}_q$ contains consecutive primitive nth roots of unity if and only if $n \neq 1, 2, 3, 6$.

Corollary

There does not exist a finite field $\mathbb{Z}_q$ with two adjacent primitive 6th roots of unity.

Main Theorem and Some Interesting Corollaries

Theorem

There exists a prime q such that $\mathbb{Z}_q$ contains consecutive primitive nth roots of unity if and only if $n \neq 1, 2, 3, 6$.

Corollary

There does not exist a finite field $\mathbb{Z}_q$ with two adjacent primitive 6th roots of unity.

Corollary

For q prime, $\mathbb{Z}_q$ has adjacent elements of odd order n if and only if $\mathbb{Z}_q$ contains adjacent elements of order $2n$.

Bounding the Relevant Prime Divisors

Definition

Let $\mathfrak{d}_n$ be the number of prime divisors $q \equiv 1 \pmod{n}$ of Γ_n, counted with multiplicity.

Bounding the Relevant Prime Divisors

Definition

Let $\mathfrak{d}_n$ be the number of prime divisors $q \equiv 1 \pmod{n}$ of Γ_n, counted with multiplicity.

Lemma

The resultant Γ_n satisfies $|\Gamma_n| \leq 3^{\varphi(n)^2}$.

Bounding the Relevant Prime Divisors

Definition

Let $\mathfrak{d}_n$ be the number of prime divisors $q \equiv 1 \pmod{n}$ of Γ_n, counted with multiplicity.

Lemma

The resultant Γ_n satisfies $|\Gamma_n| \leq 3^{\varphi(n)^2}$.

Corollary

If $q | \Gamma_n$, then $q \leq 3^{\varphi(n)^2}$.

Bounds on the Number of Relevant Prime Divisors

Proposition

The following bound holds for $\mathfrak{d}_n$:

$$\mathfrak{d}_n \leq \varphi(n)^2 \frac{\ln(3)}{\ln(n+1)}.$$

If $n = p$ is prime, we have the refined bound

$$\mathfrak{d}_p \leq (p-1)^2 \frac{\ln(3)}{\ln(2p+1)}.$$

Outline

Further Interests

Conjecture

For p a prime greater than or equal to 5, all primes $q > p$ dividing Γ_p satisfy $q \equiv 1 \pmod{p}$.

Further Interests

Conjecture

For p a prime greater than or equal to 5, all primes $q > p$ dividing Γ_p satisfy $q \equiv 1 \pmod{p}$.

Conjecture

Let $p \geq 5$ be a prime, and let q be a prime. Whenever α and $\alpha + 1$ are primitive pth roots of unity in a finite field $\mathbb{F}_{q^r}$ where $q > p$, we have $\alpha \in \mathbb{F}_q$.

Further Interests

The following proposition is the beginning of an argument towards proving our first conjecture:

Proposition

When p is prime, $N(\zeta_p - \zeta_p^j + 1) \equiv 1 \pmod{p}$ for each $1 \leq j \leq p-1$.

It is much harder to reach the same conclusion for the individual prime divisors of these norms.

Further Interests

There seems to be a nice relationship between the multiplicity of a prime divisor q of the resultant and the behavior of $\Phi_n(x)$ when considered modulo q:

Further Interests

There seems to be a nice relationship between the multiplicity of a prime divisor q of the resultant and the behavior of $\Phi_n(x)$ when considered modulo q:

Conjecture

For p prime, let k be the largest integer such that $q^k | \Gamma_p$ for some prime $q \equiv 1 \pmod{p}$. If $k < \frac{p-1}{2}$, then there exist exactly k distinct elements $\alpha_1, \ldots, \alpha_k \in \mathbb{Z}_q$ such that the order of α_i and $\alpha_i + 1$ is p for each $1 \leq i \leq k$. If $k \geq \frac{p-1}{2}$, there are exactly $\frac{p-1}{2}$ distinct elements $\alpha_1, \ldots, \alpha_{\frac{p-1}{2}} \in \mathbb{Z}_q$ such that the order of α_i and $\alpha_i + 1$ is p for each $1 \leq i \leq \frac{p-1}{2}$.

Thank You

- National Science Foundation (grant DMS-1560019)

Thank You

- National Science Foundation (grant DMS-1560019)
- Muhlenberg College for supporting the REU on which this work is based

Thank You

- National Science Foundation (grant DMS-1560019)
- Muhlenberg College for supporting the REU on which this work is based
- Organizers of MASON I