Application of EVDW to Number Theory

May 5, 2022

Quadratic Residues

Lets look at the squares mod 13:

$1^2 = 1$

$2^2 = 4$

$3^2 = 9$

$4^2 = 16 \equiv 3$

$5^2 = 25 \equiv -1 \equiv 12$

$6^2 = 36 \equiv -3 \equiv 10$

$7^2 = -1 \times -1 \times 7 \times 7 = -7 \times -7 \equiv 6 \times 6 \equiv 10.$

$8^2 = (-5)^2 \equiv 5^2 \equiv 12$

$9^2 = (-4)^2 \equiv 4^2 \equiv 3$

$10^2 \equiv (-3)^2 \equiv 3^2 \equiv 9$

$11^2 \equiv (-2)^2 \equiv 2^2 \equiv 4$

$12^2 \equiv (-1)^2 \equiv 1^2 \equiv 1$

Quadratic Residues

Lets look at the squares mod 13:

$1^2 = 1$

$2^2 = 4$

$3^2 = 9$

$4^2 = 16 \equiv 3$

$5^2 = 25 \equiv -1 \equiv 12$

$6^2 = 36 \equiv -3 \equiv 10$

$7^2 = -1 \times -1 \times 7 \times 7 = -7 \times -7 \equiv 6 \times 6 \equiv 10.$

$8^2 = (-5)^2 \equiv 5^2 \equiv 12$

$9^2 = (-4)^2 \equiv 4^2 \equiv 3$

$10^2 \equiv (-3)^2 \equiv 3^2 \equiv 9$

$11^2 \equiv (-2)^2 \equiv 2^2 \equiv 4$

$12^2 \equiv (-1)^2 \equiv 1^2 \equiv 1$

So the squares are $\{1, 3, 4, 9, 10, 12\}$

Quadratic Residues

Lets look at the squares mod 13:

$1^2 = 1$

$2^2 = 4$

$3^2 = 9$

$4^2 = 16 \equiv 3$

$5^2 = 25 \equiv -1 \equiv 12$

$6^2 = 36 \equiv -3 \equiv 10$

$7^2 = -1 \times -1 \times 7 \times 7 = -7 \times -7 \equiv 6 \times 6 \equiv 10.$

$8^2 = (-5)^2 \equiv 5^2 \equiv 12$

$9^2 = (-4)^2 \equiv 4^2 \equiv 3$

$10^2 \equiv (-3)^2 \equiv 3^2 \equiv 9$

$11^2 \equiv (-2)^2 \equiv 2^2 \equiv 4$

$12^2 \equiv (-1)^2 \equiv 1^2 \equiv 1$

So the squares are $\{1, 3, 4, 9, 10, 12\}$

3,4 are consecutive.

Quadratic Residues

Lets look at the squares mod 13:

$1^2 = 1$
$2^2 = 4$
$3^2 = 9$
$4^2 = 16 \equiv 3$
$5^2 = 25 \equiv -1 \equiv 12$
$6^2 = 36 \equiv -3 \equiv 10$
$7^2 = -1 \times -1 \times 7 \times 7 = -7 \times -7 \equiv 6 \times 6 \equiv 10.$
$8^2 = (-5)^2 \equiv 5^2 \equiv 12$
$9^2 = (-4)^2 \equiv 4^2 \equiv 3$
$10^2 \equiv (-3)^2 \equiv 3^2 \equiv 9$
$11^2 \equiv (-2)^2 \equiv 2^2 \equiv 4$
$12^2 \equiv (-1)^2 \equiv 1^2 \equiv 1$

So the squares are $\{1, 3, 4, 9, 10, 12\}$

3,4 are consecutive. Is there some p so you get 17 consec sqs?

Quadratic Residues

Lets look at the squares mod 13:

$1^2 = 1$

$2^2 = 4$

$3^2 = 9$

$4^2 = 16 \equiv 3$

$5^2 = 25 \equiv -1 \equiv 12$

$6^2 = 36 \equiv -3 \equiv 10$

$7^2 = -1 \times -1 \times 7 \times 7 = -7 \times -7 \equiv 6 \times 6 \equiv 10.$

$8^2 = (-5)^2 \equiv 5^2 \equiv 12$

$9^2 = (-4)^2 \equiv 4^2 \equiv 3$

$10^2 \equiv (-3)^2 \equiv 3^2 \equiv 9$

$11^2 \equiv (-2)^2 \equiv 2^2 \equiv 4$

$12^2 \equiv (-1)^2 \equiv 1^2 \equiv 1$

So the squares are $\{1, 3, 4, 9, 10, 12\}$

3,4 are consecutive. Is there some p so you get 17 consec sqs? Will we show YES by Extended VDW?

Quadratic Residues

Lets look at the squares mod 13:

$1^2 = 1$

$2^2 = 4$

$3^2 = 9$

$4^2 = 16 \equiv 3$

$5^2 = 25 \equiv -1 \equiv 12$

$6^2 = 36 \equiv -3 \equiv 10$

$7^2 = -1 \times -1 \times 7 \times 7 = -7 \times -7 \equiv 6 \times 6 \equiv 10.$

$8^2 = (-5)^2 \equiv 5^2 \equiv 12$

$9^2 = (-4)^2 \equiv 4^2 \equiv 3$

$10^2 \equiv (-3)^2 \equiv 3^2 \equiv 9$

$11^2 \equiv (-2)^2 \equiv 2^2 \equiv 4$

$12^2 \equiv (-1)^2 \equiv 1^2 \equiv 1$

So the squares are $\{1, 3, 4, 9, 10, 12\}$

3,4 are consecutive. Is there some p so you get 17 consec sqs?
Will we show YES by Extended VDW? Yes!

Easy NT Lemma (Proof Omitted)

Def
SQ_p is the set of all nonzero squares mod p.
NSQ_p is the set of all nonzero nonsquares mod p.
Lemma Let p be a prime. All arithmetic in this problem is mod p.
Let $x, y \in \{1, \ldots, p-1\}$.

Easy NT Lemma (Proof Omitted)

Def
SQ_p is the set of all nonzero squares mod p.
NSQ_p is the set of all nonzero nonsquares mod p.
Lemma Let p be a prime. All arithmetic in this problem is mod p.
Let $x, y \in \{1, \ldots, p-1\}$.

1. If $x, y \in \mathrm{SQ}_p$ then $xy \in \mathrm{SQ}_p$.

Easy NT Lemma (Proof Omitted)

Def
SQ_p is the set of all nonzero squares mod p.
NSQ_p is the set of all nonzero nonsquares mod p.
Lemma Let p be a prime. All arithmetic in this problem is mod p.
Let $x, y \in \{1, \ldots, p-1\}$.

1. If $x, y \in \mathrm{SQ}_p$ then $xy \in \mathrm{SQ}_p$.
2. If $x \in \mathrm{NSQ}_p$ and $y \in \mathrm{SQ}_p$ then $xy \in \mathrm{NSQ}_p$.

Easy NT Lemma (Proof Omitted)

Def
SQ_p is the set of all nonzero squares mod p.
NSQ_p is the set of all nonzero nonsquares mod p.
Lemma Let p be a prime. All arithmetic in this problem is mod p.
Let $x, y \in \{1, \ldots, p-1\}$.

1. If $x, y \in \mathrm{SQ}_p$ then $xy \in \mathrm{SQ}_p$.
2. If $x \in \mathrm{NSQ}_p$ and $y \in \mathrm{SQ}_p$ then $xy \in \mathrm{NSQ}_p$.
3. If $x \in \mathrm{SQ}_p$ then $x^{-1} \in \mathrm{SQ}_p$.

Basic Number Theory Lemma

Lemma

Basic Number Theory Lemma

Lemma

1. $|\mathrm{SQ}_p| = |\mathrm{NSQ}_p| = \frac{p-1}{2}$.

Basic Number Theory Lemma

Lemma

1. $|\mathrm{SQ}_p| = |\mathrm{NSQ}_p| = \frac{p-1}{2}$.
2. If $x \in \{1, \ldots, p-1\}$ then $x \cdot \{1, \ldots, p-1\} = \{1, \ldots, p-1\}$

Basic Number Theory Lemma

Lemma

1. $|\mathrm{SQ}_p| = |\mathrm{NSQ}_p| = \frac{p-1}{2}$.
2. If $x \in \{1, \ldots, p-1\}$ then $x \cdot \{1, \ldots, p-1\} = \{1, \ldots, p-1\}$

Pf

Basic Number Theory Lemma

Lemma

1. $|\mathrm{SQ}_p| = |\mathrm{NSQ}_p| = \frac{p-1}{2}$.
2. If $x \in \{1, \ldots, p-1\}$ then $x \cdot \{1, \ldots, p-1\} = \{1, \ldots, p-1\}$

Pf

1) The map $x \rightarrow x^2$ is 2-to-1.

Basic Number Theory Lemma

Lemma

1. $|\mathrm{SQ}_p| = |\mathrm{NSQ}_p| = \frac{p-1}{2}$.
2. If $x \in \{1, \ldots, p-1\}$ then
   $x \cdot \{1, \ldots, p-1\} = \{1, \ldots, p-1\}$

Pf

1) The map $x \rightarrow x^2$ is 2-to-1.

2) Given z want a y such that $xy \equiv z$. Just take $y = x^{-1}z$.

Basic Number Theory Lemma

Lemma

1. $|\mathrm{SQ}_p| = |\mathrm{NSQ}_p| = \frac{p-1}{2}$.
2. If $x \in \{1, \ldots, p-1\}$ then
   $x \cdot \{1, \ldots, p-1\} = \{1, \ldots, p-1\}$

Pf

1) The map $x \rightarrow x^2$ is 2-to-1.

2) Given z want a y such that $xy \equiv z$. Just take $y = x^{-1}z$.

End of Pf

Interesting NT Lemma

Lemma

Interesting NT Lemma

Lemma

1) If $x, y \in \mathrm{NSQ}_p$ then $xy \in \mathrm{SQ}_p$.

Interesting NT Lemma

Lemma

1) If $x, y \in \mathrm{NSQ}_p$ then $xy \in \mathrm{SQ}_p$.
2) If $x \in \mathrm{NSQ}_p$ then $x^{-1} \in \mathrm{NSQ}_p$ (proof omitted).

Interesting NT Lemma

Lemma

1) If $x, y \in \mathrm{NSQ}_p$ then $xy \in \mathrm{SQ}_p$.
2) If $x \in \mathrm{NSQ}_p$ then $x^{-1} \in \mathrm{NSQ}_p$ (proof omitted).

Pf

Let $x \in \mathrm{NSQ}_p$.

Interesting NT Lemma

Lemma

1) If $x, y \in \mathrm{NSQ}_p$ then $xy \in \mathrm{SQ}_p$.
2) If $x \in \mathrm{NSQ}_p$ then $x^{-1} \in \mathrm{NSQ}_p$ (proof omitted).

Pf

Let $x \in \mathrm{NSQ}_p$.

Recall that $x \cdot \{1, 2, \ldots, p-1\} = \{1, \ldots, p-1\}$. So

Interesting NT Lemma

Lemma

1) If $x, y \in \mathrm{NSQ}_p$ then $xy \in \mathrm{SQ}_p$.
2) If $x \in \mathrm{NSQ}_p$ then $x^{-1} \in \mathrm{NSQ}_p$ (proof omitted).

Pf

Let $x \in \mathrm{NSQ}_p$.

Recall that $x \cdot \{1, 2, \ldots, p-1\} = \{1, \ldots, p-1\}$. So

$(x \cdot \mathrm{SQ}_p) \cup (x \cdot \mathrm{NSQ}_p) = \{1, \ldots, p-1\}$.

Interesting NT Lemma

Lemma

1) If $x, y \in \mathrm{NSQ}_p$ then $xy \in \mathrm{SQ}_p$.
2) If $x \in \mathrm{NSQ}_p$ then $x^{-1} \in \mathrm{NSQ}_p$ (proof omitted).

Pf

Let $x \in \mathrm{NSQ}_p$.

Recall that $x \cdot \{1, 2, \ldots, p-1\} = \{1, \ldots, p-1\}$. So

$(x \cdot \mathrm{SQ}_p) \cup (x \cdot \mathrm{NSQ}_p) = \{1, \ldots, p-1\}$.

$x \cdot \mathrm{SQ}_p = \mathrm{NSQ}_p$. Hence $x \cdot \mathrm{NSQ}_p = \mathrm{SQ}_p$.

Interesting NT Lemma

Lemma
1) If $x, y \in \mathrm{NSQ}_p$ then $xy \in \mathrm{SQ}_p$.
2) If $x \in \mathrm{NSQ}_p$ then $x^{-1} \in \mathrm{NSQ}_p$ (proof omitted).
Pf
Let $x \in \mathrm{NSQ}_p$.

Recall that $x \cdot \{1, 2, \ldots, p-1\} = \{1, \ldots, p-1\}$. So

$(x \cdot \mathrm{SQ}_p) \cup (x \cdot \mathrm{NSQ}_p) = \{1, \ldots, p-1\}$.

$x \cdot \mathrm{SQ}_p = \mathrm{NSQ}_p$. Hence $x \cdot \mathrm{NSQ}_p = \mathrm{SQ}_p$.
End of Pf

Lemma We Will use in Main Theorem

Def Let p be a prime and $x, y \in \{1, \ldots, p-1\}$. x and y are **of the same type** if either $x, y \in \mathrm{SQ}_p$ or $x, y \in \mathrm{NSQ}_p$.

Lemma We Will use in Main Theorem

Def Let p be a prime and $x, y \in \{1, \ldots, p-1\}$. x and y are **of the same type** if either $x, y \in \mathrm{SQ}_p$ or $x, y \in \mathrm{NSQ}_p$.

Lemma Let p be a prime and $x, y \in \{1, \ldots, p-1\}$. If x, y are of the same type then

Lemma We Will use in Main Theorem

Def Let p be a prime and $x, y \in \{1, \ldots, p-1\}$. x and y are **of the same type** if either $x, y \in \mathrm{SQ}_p$ or $x, y \in \mathrm{NSQ}_p$.

Lemma Let p be a prime and $x, y \in \{1, \ldots, p-1\}$. If x, y are of the same type then
1) $xy \in \mathrm{SQ}_p$.

Lemma We Will use in Main Theorem

Def Let p be a prime and $x, y \in \{1, \ldots, p-1\}$. x and y are **of the same type** if either $x, y \in \mathrm{SQ}_p$ or $x, y \in \mathrm{NSQ}_p$.

Lemma Let p be a prime and $x, y \in \{1, \ldots, p-1\}$. If x, y are of the same type then
1) $xy \in \mathrm{SQ}_p$.
2) $x^{-1}y \in \mathrm{SQ}_p$.

Main Theorem

Thm $(\forall k)(\exists p)$ there are k consecutive squares mod p.
Pf We determine p later. We color $[p-1]$ as follows:

Main Theorem

Thm $(\forall k)(\exists p)$ there are k consecutive squares mod p.
Pf We determine p later. We color $[p-1]$ as follows:

$$\mathrm{COL}(x) = \begin{cases} R & \text{if } x \in \mathrm{SQ}_p \\ B & \text{if } x \in \mathrm{NSQ}_p \end{cases} \tag{1}$$

Main Theorem

Thm $(\forall k)(\exists p)$ there are k consecutive squares mod p.
Pf We determine p later. We color $[p-1]$ as follows:

$$\mathrm{COL}(x) = \begin{cases} R & \text{if } x \in \mathrm{SQ}_p \\ B & \text{if } x \in \mathrm{NSQ}_p \end{cases} \tag{1}$$

By EVDW There exists a, d such that
$a, a+d, a+2d, \ldots, a+(K-1)d$ and d are all the same

Main Theorem

Thm $(\forall k)(\exists p)$ there are k consecutive squares mod p.
Pf We determine p later. We color $[p-1]$ as follows:

$$\mathrm{COL}(x) = \begin{cases} R & \text{if } x \in \mathrm{SQ}_p \\ B & \text{if } x \in \mathrm{NSQ}_p \end{cases} \tag{1}$$

By EVDW There exists a, d such that
$a, a+d, a+2d, \ldots, a+(K-1)d$ and d are all the same **type**.

Main Theorem

Thm $(\forall k)(\exists p)$ there are k consecutive squares mod p.
Pf We determine p later. We color $[p-1]$ as follows:

$$\mathrm{COL}(x) = \begin{cases} R & \text{if } x \in \mathrm{SQ}_p \\ B & \text{if } x \in \mathrm{NSQ}_p \end{cases} \tag{1}$$

By EVDW There exists a, d such that
$a, a+d, a+2d, \ldots, a+(K-1)d$ and d are all the same **type**.

By Lemma
$ad^{-1}, (a+d)d^{-1}, \ldots, (a+(K-1)d)d^{-1} \in \mathrm{SQ}_p$.

Main Theorem

Thm $(\forall k)(\exists p)$ there are k consecutive squares mod p.
Pf We determine p later. We color $[p-1]$ as follows:

$$\mathrm{COL}(x) = \begin{cases} R & \text{if } x \in \mathrm{SQ}_p \\ B & \text{if } x \in \mathrm{NSQ}_p \end{cases} \tag{1}$$

By EVDW There exists a, d such that
$a, a+d, a+2d, \ldots, a+(K-1)d$ and d are all the same **type**.

By Lemma
$ad^{-1}, (a+d)d^{-1}, \ldots, (a+(K-1)d)d^{-1} \in \mathrm{SQ}_p$.
$ad^{-1}, ad^{-1}+1, \ldots, ad^{-1}+K-1 \in \mathrm{SQ}_p$.

Main Theorem

Thm $(\forall k)(\exists p)$ there are k consecutive squares mod p.
Pf We determine p later. We color $[p-1]$ as follows:

$$\mathrm{COL}(x) = \begin{cases} R & \text{if } x \in \mathrm{SQ}_p \\ B & \text{if } x \in \mathrm{NSQ}_p \end{cases} \quad (1)$$

By EVDW There exists a, d such that
$a, a+d, a+2d, \ldots, a+(K-1)d$ and d are all the same **type**.

By Lemma
$ad^{-1}, (a+d)d^{-1}, \ldots, (a+(K-1)d)d^{-1} \in \mathrm{SQ}_p$.
$ad^{-1}, ad^{-1}+1, \ldots, ad^{-1}+K-1 \in \mathrm{SQ}_p$.
Take K large enough so even if get wrap around, get k consecutive.