An easy proof of quadratic reciprocity

Brant Jones
jones3bc@jmu.edu
James Madison University

January 16, 2019

What is quadratic reciprocity about?

Throughout this talk, let p and q be odd primes...

Let $\chi_p(q)$ be 1 or -1 according to whether q **is** or **is not** a perfect square mod p.

Example. Working mod 5, $1 = 1^2 = 4^2$, $4 = 2^2 = 3^2$.
Example. Working mod 7, 5 is not a perfect square.
Example. Working mod 11, $5 = 4^2 = 7^2$.
Example. Working mod 13, or mod 17, 5 is not a perfect square.
Example. Working mod 19, $5 = 9^2 = 10^2$.

What is quadratic reciprocity about?

Throughout this talk, let p and q be odd primes. . .

Let $\chi_p(q)$ be 1 or -1 according to whether q **is** or **is not** a perfect square mod p.

Example. Working mod 5, $1 = 1^2 = 4^2$, $4 = 2^2 = 3^2$.
Example. Working mod 7, 5 is not a perfect square.
Example. Working mod 11, $5 = 4^2 = 7^2$.
Example. Working mod 13, or mod 17, 5 is not a perfect square.
Example. Working mod 19, $5 = 9^2 = 10^2$.

What is quadratic reciprocity about?

Throughout this talk, let p and q be odd primes. . .

Let $\chi_p(q)$ be 1 or -1 according to whether q **is** or **is not** a perfect square mod p.

Example. Working mod 5, $1 = 1^2 = 4^2$, $4 = 2^2 = 3^2$.
Example. Working mod 7, 5 is not a perfect square.
Example. Working mod 11, $5 = 4^2 = 7^2$.
Example. Working mod 13, or mod 17, 5 is not a perfect square.
Example. Working mod 19, $5 = 9^2 = 10^2$.

What is quadratic reciprocity about?

Throughout this talk, let p and q be odd primes. . .

Let $\chi_p(q)$ be 1 or -1 according to whether q **is** or **is not** a perfect square mod p.

Example. Working mod 5, $1 = 1^2 = 4^2$, $4 = 2^2 = 3^2$.
Example. Working mod 7, 5 is not a perfect square.
Example. Working mod 11, $5 = 4^2 = 7^2$.
Example. Working mod 13, or mod 17, 5 is not a perfect square.
Example. Working mod 19, $5 = 9^2 = 10^2$.

What is quadratic reciprocity about?

Throughout this talk, let p and q be odd primes. . .

Let $\chi_p(q)$ be 1 or -1 according to whether q **is** or **is not** a perfect square mod p.

Example. Working mod 5, $1 = 1^2 = 4^2$, $4 = 2^2 = 3^2$.
Example. Working mod 7, 5 is not a perfect square.
Example. Working mod 11, $5 = 4^2 = 7^2$.
Example. Working mod 13, or mod 17, 5 is not a perfect square.
Example. Working mod 19, $5 = 9^2 = 10^2$.

What is quadratic reciprocity about?

Throughout this talk, let p and q be odd primes. . .

Let $\chi_p(q)$ be 1 or -1 according to whether q **is** or **is not** a perfect square mod p.

Example. Working mod 5, $1 = 1^2 = 4^2$, $4 = 2^2 = 3^2$.
Example. Working mod 7$\equiv$ 2 mod 5, 5 is not a perfect square.
Example. Working mod 11$\equiv$ 1 mod 5, $5 = 4^2 = 7^2$.
Example. Working mod 13$\equiv$ 3 mod 5, or mod 17$\equiv$ 2 mod 5, 5 is not a perfect square.
Example. Working mod 19$\equiv$ 4 mod 5, $5 = 9^2 = 10^2$.
After studying such data, you may imagine that $\chi_p(q) = \chi_q(p)$.
Actually, there is one more rule: $\chi_p(q) = -\chi_q(p)$ if p and q are both 3 mod 4.

What is quadratic reciprocity about?

Throughout this talk, let p and q be odd primes. . .

Let $\chi_p(q)$ be 1 or -1 according to whether q **is** or **is not** a perfect square mod p.

Example. Working mod 5, $1 = 1^2 = 4^2$, $4 = 2^2 = 3^2$.
Example. Working mod 7$\equiv$ 2 mod 5, 5 is not a perfect square.
Example. Working mod 11$\equiv$ 1 mod 5, $5 = 4^2 = 7^2$.
Example. Working mod 13$\equiv$ 3 mod 5, or mod 17$\equiv$ 2 mod 5, 5 is not a perfect square.
Example. Working mod 19$\equiv$ 4 mod 5, $5 = 9^2 = 10^2$.
After studying such data, you may imagine that $\chi_p(q) = \chi_q(p)$.
Actually, there is one more rule: $\chi_p(q) = -\chi_q(p)$ if p and q are both 3 mod 4.

Reformulation

Theorem

(Euler's criterion) *For any odd prime p,* $\chi_p(q) = q^{\frac{p-1}{2}} \bmod p$

- Fermat's Little Theorem proves $q^{\frac{p-1}{2}} \bmod p$ is ± 1:
  p divides $(q^{p-1} - 1) = (q^{\frac{p-1}{2}} - 1)(q^{\frac{p-1}{2}} + 1)$ so divides one of the factors.
- Existence of primitive roots mod p proves the correspondence with $\chi_p(q)$.

So, we can restate QR as saying that we have the following **equality of signs**:

$$\left(q^{\frac{p-1}{2}} \bmod p\right)\left(p^{\frac{q-1}{2}} \bmod q\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

(where the RHS is -1 precisely if p and q are both 3 mod 4.)

So how to prove

$$\left(q^{\frac{p-1}{2}} \bmod p\right)\left(p^{\frac{q-1}{2}} \bmod q\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}?$$

- We need a common setting where we can work mod p and mod q … **Chinese Remainder Theorem**:

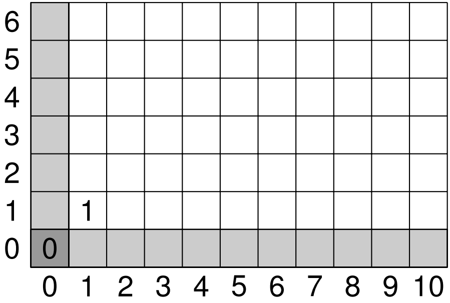
  $$\mathbb{Z}_{pq} \equiv \mathbb{Z}_p \times \mathbb{Z}_q$$

  and moreover

  $$\mathbb{Z}_{pq}^{\perp} \equiv \mathbb{Z}_p^{\perp} \times \mathbb{Z}_q^{\perp}$$

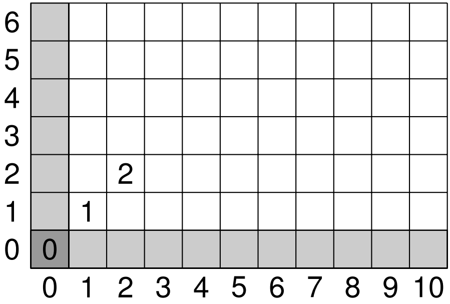
  where $\mathbb{Z}_{pq}^{\perp}$ is the set of classes **relatively prime** to pq**.**
- The statement is about comparing signs, so we should set up some **products that are off by a sign** …

CRT by picture



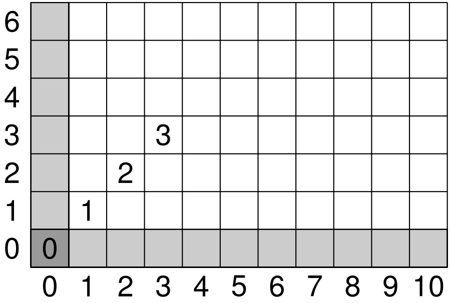
- Label by integers along the diagonal line $y = x$ using torus/“pacman” rules to wrap around.

CRT by picture



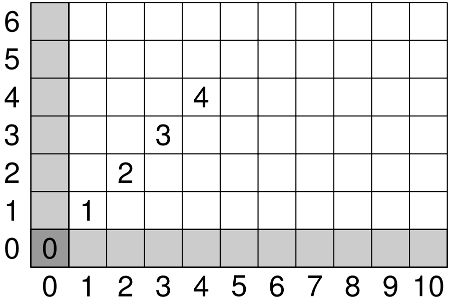
- Label by integers along the diagonal line $y = x$ using torus/“pacman” rules to wrap around.

CRT by picture



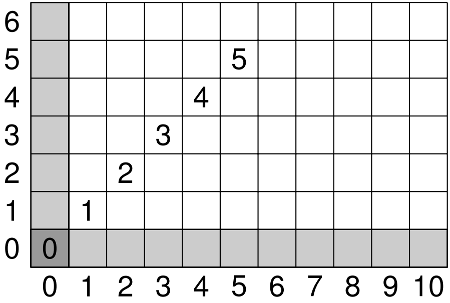
- Label by integers along the diagonal line $y = x$ using torus/“pacman” rules to wrap around.

CRT by picture



- Label by integers along the diagonal line $y = x$ using torus/“pacman” rules to wrap around.

CRT by picture



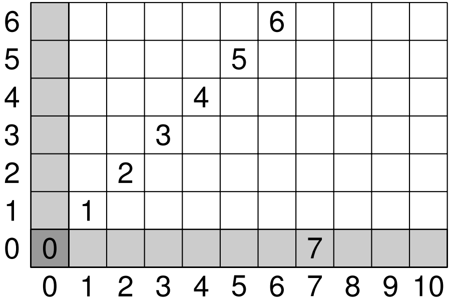
- Label by integers along the diagonal line $y = x$ using torus/"pacman" rules to wrap around.

CRT by picture

6							6				
5						5					
4					4						
3				3							
2			2								
1		1									
0	0										
	0	1	2	3	4	5	6	7	8	9	10

- Label by integers along the diagonal line $y = x$ using torus/“pacman” rules to wrap around.

CRT by picture



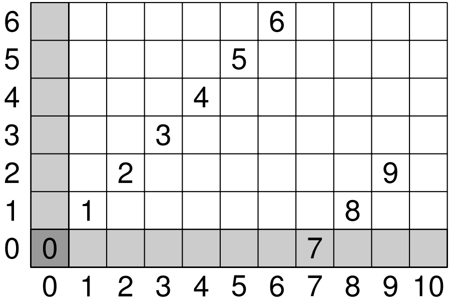
- Label by integers along the diagonal line $y = x$ using torus/“pacman” rules to wrap around.

CRT by picture

6							6				
5						5					
4					4						
3				3							
2			2								
1		1							8		
0	0							7			
	0	1	2	3	4	5	6	7	8	9	10

- Label by integers along the diagonal line $y = x$ using torus/“pacman” rules to wrap around.

CRT by picture



- Label by integers along the diagonal line $y = x$ using torus/“pacman” rules to wrap around.

CRT by picture

6							6				
5						5					
4					4						
3				3							10
2			2							9	
1		1							8		
0	0							7			
	0	1	2	3	4	5	6	7	8	9	10

- Label by integers along the diagonal line $y = x$ using torus/“pacman” rules to wrap around.

CRT by picture

6							6				
5						5					
4	11				4						
3				3							10
2			2							9	
1		1							8		
0	0							7			
	0	1	2	3	4	5	6	7	8	9	10

- Label by integers along the diagonal line $y = x$ using torus/“pacman” rules to wrap around.

CRT by picture

6							6				
5		12				5					
4	11				4						
3				3							10
2			2							9	
1		1							8		
0	0							7			
	0	1	2	3	4	5	6	7	8	9	10

- Label by integers along the diagonal line $y = x$ using torus/“pacman” rules to wrap around.

CRT by picture

6	55	34	13	69	48	27	6	62	41	20	76
5	33	12	68	47	26	5	61	40	19	75	54
4	11	67	46	25	4	60	39	18	74	53	32
3	66	45	24	3	59	38	17	73	52	31	10
2	44	23	2	58	37	16	72	51	30	9	65
1	22	1	57	36	15	71	50	29	8	64	43
0	0	56	35	14	70	49	28	7	63	42	21
	0	1	2	3	4	5	6	7	8	9	10

- Label by integers along the diagonal line $y = x$ using torus/“pacman” rules to wrap around.
- Labeling (by $\mathbb{Z}_{pq}$ or $\mathbb{Z}_{pq}^{\perp}$) is injective, by uniqueness of prime factorization.

CRT by picture

6	55	34	13	69	48	27	6	62	41	20	76
5	33	12	68	47	26	5	61	40	19	75	54
4	11	67	46	25	4	60	39	18	74	53	32
3	66	45	24	3	59	38	17	73	52	31	10
2	44	23	2	58	37	16	72	51	30	9	65
1	22	1	57	36	15	71	50	29	8	64	43
0	0	56	35	14	70	49	28	7	63	42	21
	0	1	2	3	4	5	6	7	8	9	10

- Label by integers along the diagonal line $y = x$ using torus/“pacman” rules to wrap around.
- Labeling (by $\mathbb{Z}_{pq}$ or $\mathbb{Z}_{pq}^{\perp}$) is injective, by uniqueness of prime factorization.
- **Multiplication by** -1 is reflection through the lines at $\frac{p-1}{2}$ and $\frac{q-1}{2}$.

Say a subset $S \subseteq \mathbb{Z}_{pq}^{\perp}$ is **anti-symmetric** if for each $i \in \mathbb{Z}_{pq}^{\perp}$, we have precisely one of i or $-i$ in S:

6		34	13			27	6			20	
5		12			26	5			19		
4				25	4			18			32
3			24	3		38	17			31	10
2		23	2		37	16			30	9	
1		1		36	15			29	8		
0											
	0	1	2	3	4	5	6	7	8	9	10

6		34	13	69	48	27					
5		12	68	47	26	5					
4		67	46	25	4	60					
3		45	24	3	59	38					
2		23	2	58	37	16					
1		1	57	36	15	71					
0											
	0	1	2	3	4	5	6	7	8	9	10

6											
5											
4											
3		45	24	3	59	38	17	73	52	31	10
2		23	2	58	37	16	72	51	30	9	65
1		1	57	36	15	71	50	29	8	64	43
0											
	0	1	2	3	4	5	6	7	8	9	10

Notice the sign change required to move between the lower two sets is RHS of our QR statement: $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Say a subset $S \subseteq \mathbb{Z}_{pq}^{\perp}$ is **anti-symmetric** if for each $i \in \mathbb{Z}_{pq}^{\perp}$, we have precisely one of i or $-i$ in S:

6		34	13			27	6			20	
5		12			26	5			19		
4				25	4			18			32
3			24	3		38	17			31	10
2		23	2		37	16			30	9	
1		1		36	15			29	8		
0											
	0	1	2	3	4	5	6	7	8	9	10

6		34	13	69	48	27					
5		12	68	47	26	5					
4		67	46	25	4	60					
3		45	24	3	59	38					
2		23	2	58	37	16					
1		1	57	36	15	71					
0											
	0	1	2	3	4	5	6	7	8	9	10

6											
5											
4											
3		45	24	3	59	38	17	73	52	31	10
2		23	2	58	37	16	72	51	30	9	65
1		1	57	36	15	71	50	29	8	64	43
0											
	0	1	2	3	4	5	6	7	8	9	10

Notice the sign change required to move between the lower two sets is RHS of our QR statement: $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Say a subset $S \subseteq \mathbb{Z}_{pq}^{\perp}$ is **anti-symmetric** if for each $i \in \mathbb{Z}_{pq}^{\perp}$, we have precisely one of i or $-i$ in S:

6		34	13			27	6			20	
5		12			26	5			19		
4				25	4			18			32
3			24	3		38	17			31	10
2		23	2		37	16			30	9	
1		1		36	15			29	8		
0											
	0	1	2	3	4	5	6	7	8	9	10

6		34	13	69	48	27					
5		12	68	47	26	5					
4		67	46	25	4	60					
3		45	24	3	59	38					
2		23	2	58	37	16					
1		1	57	36	15	71					
0											
	0	1	2	3	4	5	6	7	8	9	10

6											
5											
4											
3		45	24	3	59	38	17	73	52	31	10
2		23	2	58	37	16	72	51	30	9	65
1		1	57	36	15	71	50	29	8	64	43
0											
	0	1	2	3	4	5	6	7	8	9	10

Notice the sign change required to move between the lower two sets is RHS of our QR statement: $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Sign change via the upper set?

Compare the product of these residues mod p (horizontal):

6											
5											
4											
3		45	24	3	59	38	17	73	52	31	10
2		23	2	58	37	16	72	51	30	9	65
1		1	57	36	15	71	50	29	8	64	43
0											
	0	1	2	3	4	5	6	7	8	9	10

$$(p-1)!^{\frac{q-1}{2}} \bmod p$$

Last entry: $\frac{pq-1}{2}$. Working mod p: $\frac{pq-p+p-1}{2} = p\frac{q-1}{2} + \frac{p-1}{2}$.

Hence, last multiple of q is: $\frac{pq-q+q-1}{2} = q\frac{p-1}{2} + \frac{q-1}{2}$.

6		34	13			27	6			20	
5		12			26	5			19		
4				25	4			18			32
3			24	3		38	17			31	10
2		23	2		37	16			30	9	
1		1		36	15			29	8		
0			35	14			28	7			21
	0	1	2	3	4	5	6	7	8	9	10

$$\frac{(p-1)!^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)!}{q(2q)\cdots\left(\frac{p-1}{2}q\right)} \bmod p$$

So: the **sign change** is $q^{\frac{p-1}{2}}$ mod p.

Sign change via the upper set?

Compare the product of these residues mod p (horizontal):

6											
5											
4											
3		45	24	3	59	38	17	73	52	31	10
2		23	2	58	37	16	72	51	30	9	65
1		1	57	36	15	71	50	29	8	64	43
0											
	0	1	2	3	4	5	6	7	8	9	10

$$(p-1)!^{\frac{q-1}{2}} \bmod p$$

Last entry: $\frac{pq-1}{2}$. Working mod p: $\frac{pq-p+p-1}{2} = p\frac{q-1}{2} + \frac{p-1}{2}$.

Hence, last multiple of q is: $\frac{pq-q+q-1}{2} = q\frac{p-1}{2} + \frac{q-1}{2}$.

6		34	13			27	6			20	
5		12			26	5			19		
4				25	4			18			32
3			24	3		38	17			31	10
2		23	2		37	16			30	9	
1		1		36	15			29	8		
0			35	14			28	7			21
	0	1	2	3	4	5	6	7	8	9	10

$$\frac{(p-1)!^{\frac{q-1}{2}}\left(\frac{p-1}{2}\right)!}{q(2q)\cdots\left(\frac{p-1}{2}q\right)} \bmod p$$

So: the **sign change** is $q^{\frac{p-1}{2}} \bmod p$.

Sign change via the upper set?

Compare the product of these residues mod p (horizontal):

6											
5											
4											
3		45	24	3	59	38	17	73	52	31	10
2		23	2	58	37	16	72	51	30	9	65
1		1	57	36	15	71	50	29	8	64	43
0											
	0	1	2	3	4	5	6	7	8	9	10

$$(p-1)!^{\frac{q-1}{2}} \bmod p$$

Last entry: $\frac{pq-1}{2}$. Working mod p: $\frac{pq-p+p-1}{2} = p\frac{q-1}{2} + \frac{p-1}{2}$.

Hence, last multiple of q is: $\frac{pq-q+q-1}{2} = q\frac{p-1}{2} + \frac{q-1}{2}$.

6		34	13			27	6			20	
5		12			26	5			19		
4				25	4			18			32
3			24	3		38	17			31	10
2		23	2		37	16			30	9	
1		1		36	15			29	8		
0			35	14			28	7			21
	0	1	2	3	4	5	6	7	8	9	10

$$\frac{(p-1)!^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)!}{q(2q)\cdots\left(\frac{p-1}{2}q\right)} \bmod p$$

So: the **sign change** is $q^{\frac{p-1}{2}}$ mod p.

Sign change via the upper set?

Compare the product of these residues mod p (horizontal):

6											
5											
4											
3		45	24	3	59	38	17	73	52	31	10
2		23	2	58	37	16	72	51	30	9	65
1		1	57	36	15	71	50	29	8	64	43
0											
	0	1	2	3	4	5	6	7	8	9	10

$$(p-1)!^{\frac{q-1}{2}} \bmod p$$

Last entry: $\frac{pq-1}{2}$. Working mod p: $\frac{pq-p+p-1}{2} = p\frac{q-1}{2} + \frac{p-1}{2}$.

Hence, last multiple of q is: $\frac{pq-q+q-1}{2} = q\frac{p-1}{2} + \frac{q-1}{2}$.

6		34	13			27	6			20	
5		12			26	5			19		
4				25	4			18			32
3			24	3		38	17			31	10
2		23	2		37	16			30	9	
1		1		36	15			29	8		
0			35	14			28	7			21
	0	1	2	3	4	5	6	7	8	9	10

$$\frac{(p-1)!^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)!}{q(2q)\cdots\left(\frac{p-1}{2}q\right)} \bmod p$$

So: the **sign change** is $q^{\frac{p-1}{2}} \bmod p$.

Quadratic Reciprocity by picture!

	0	1	2	3	4	5	6	7	8	9	10
6		34	13			27	6			20	
5		12			26	5			19		
4				25	4			18			32
3			24	3		38	17			31	10
2		23	2		37	16			30	9	
1		1		36	15			29	8		
0											

$p^{\frac{q-1}{2}} \bmod q$

$q^{\frac{p-1}{2}} \bmod p$

	0	1	2	3	4	5	6	7	8	9	10
6		34	13	69	48	27					
5		12	68	47	26	5					
4		67	46	25	4	60					
3		45	24	3	59	38					
2		23	2	58	37	16					
1		1	57	36	15	71					
0											

	0	1	2	3	4	5	6	7	8	9	10
6											
5											
4											
3		45	24	3	59	38	17	73	52	31	10
2		23	2	58	37	16	72	51	30	9	65
1		1	57	36	15	71	50	29	8	64	43
0											

$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

Sources

mathoverflow

Questions Tags Users Badges

What's the "best" proof of quadratic reciprocity?

74

For my purposes, you may want to interpret "best" as "clearest and easiest to understand for undergrads in a first number theory course," but don't feel too constrained.

nt.number-theory big-list quadratic-reciprocity

share cite improve this question edited Apr 10 '15 at 12:43 community wiki 2 revs, 2 users 100% Ben Webster

97

- Gauss proof V
- G. Rousseau, On the Quadratic Reciprocity Law, J. Austral. Math. Soc. Ser. A 51 (1991), no. 3, 423-–425.
- Tim Kunisky, Quadratic Reciprocity by Group Theory, Harvard College Math. Review, Vol. 2, no. 2 (2008), 75-–76.