L11 Quadratic residues (and non-residues)

Corollary $p>2$, then $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}1 \dots p\equiv 1(4),\\ -1 \dots p\equiv 3(4).\end{cases}$

Proof. By Euler's criterion, $\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}} \pmod p$ but since both sides are ± 1 and $p>2$, this holds even as an equality. ☒

For $p>2$, we consider two complete systems of residues (modulo p ($\neq 0$)): $R_p=\{1,2,\dots,p-1\}$ and $N_p=\{-\frac{p-1}{2},-\frac{p+1}{2},\dots,-1,1,2\dots,\frac{p-1}{2}\}$. Further let $R_p^-=\{1,2,\dots,\frac{p-1}{2}\}$, $R_p^+=\{\frac{p+1}{2},\frac{p+3}{2},\dots,p-1\}$, $N_p^-=\{-\frac{p-1}{2},\dots,-1\}$ and $N_p^+=\{1,2,\dots,\frac{p-1}{2}\}$. For $a\in\mathbb{Z}$, $a\not\equiv 0(p)$ we define $n(a)=(n_q \mid n_q\in R_p, n_q\equiv qa(p), q=1,2,\dots,\frac{p-1}{2})$

($n(a)=$ —"— N_p —"—)

$n(a)^+$, resp. $n(a)^-$, are the terms in $n(a)$ lying in R_p^+, resp. in N_p^-, and similarly for $n(a)^+$ and $n(a)^-$.

Example $p=11$, $a=6$, $n(a)=(6,1,7,2,8)$, $n(a)=(-5,1,-4,2,-3)$, $n(a)^+=(6,7,8)$, $n(6)^-=(1,2)$, $n(6)^+=(1,2)$, $n(6)^-=(-5,-4,-3)$.

The order really does not matter, and we will be interested mostly in the cardinalities of the sequences/sets $n(a)^\pm$, $n(a)^\pm$.

1. (Observation) $m(a)^- = n(a)^+$, $m(a)^+ = p = n(a)^\circ$, hence (for cardinalities) $|m(a)^-| = |n(a)^+|$ & $|m(a)^+| = |n(a)^-|$.

2. $n(a)^\circ$ (minus signs deleted) = a permutation of $\{1, 2, \dots, \frac{p-1}{2}\}$
Similarly, $m(a)^\circ$ ($x \in m(a)^+$ replaced with $p - x$) $= n(a)^-$.

Theorem (Gauss's lemma)

$$\left(\frac{a}{p}\right) = (-1)^{|m(a)^+|} = (-1)^{|n(a)^-|}.$$

Proof - Because of the 1st observ. it suffices to prove just that $\left(\frac{a}{p}\right) \equiv (-1)^{|n(a)^-|}$ modulo p:

$$\frac{p-1}{2}! \; a^{\frac{p-1}{2}} = \prod_{q=1}^{\frac{p-1}{2}} qa \equiv \prod x = (-1)^{|m(a)^-|} \cdot \frac{p-1}{2}!$$

($x \in n(a)$; the $\equiv$: by the def. of $n(a)$; the $=$: by the 2nd observ. and the def. of $n(a)^-$)

$\rightsquigarrow a^{\frac{p-1}{2}} \equiv (-1)^{|n(a)^-|} \pmod p \rightsquigarrow$ (by Euler's crit.)

$\rightsquigarrow \left(\frac{a}{p}\right) \equiv (-1)^{|n(a)^-|} \overset{-1,0,1}{\rightsquigarrow} \left(\frac{a}{p}\right) = (-1)^{|n(a)^-|}$. ☒

2nd $\quad p > 2$

Proposition (Supplements to the QRL) $p > 2$:

a (the 1st suppl. is the above formula for $\left(\frac{-1}{p}\right)$)

$$\left(\frac{2}{p}\right) = \begin{cases} 1 \dots p \equiv 1, 7 \pmod 8 \\ -1 \dots p \equiv 3, 5 \; (-11-) \end{cases} \left(= (-1)^{\frac{p^2-1}{8}} \right)$$

Proof. For given prime $p>2$, by Gauss's lemma we ha
ve that $\left(\frac{2}{p}\right) = (-1)^{|M(q)^+|}$. But $|M(q)^+|$ = the # of
$q \in \{1,2,\dots,\frac{p-1}{2}\}$ s.t. $\frac{p+1}{2} \le 2q \le p-1$ (no reduction mod p) =
$= \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor$ = for $p = 8r+s$ = $4r + \frac{s-1}{2} - \left\lfloor 2r + \frac{s-1}{4} \right\rfloor \equiv$
... s.t. $1 \le 2q \le \frac{p-1}{2}$ $\quad$ $1,3,5,7$

$\equiv \pmod 2$ $\quad \frac{s-1}{2} - \left\lfloor \frac{s-1}{4} \right\rfloor = \begin{cases} 0 \dots s=1 \\ 1 \dots s=3 \\ 1 \dots s=5 \\ 2 \dots s=7 \end{cases}$ $\quad \square$

QRL = the Quadratic Reciprocity Law, first proved by C.F. Gauss, but known to Euler or Legendre earlier. Gauss called it "Theorema Aureum" (golden theorem)

For $p,q>2$, $p \neq q$: $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$.

Explicitly $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ ... $p \equiv 1 (4)$ or $q \equiv 1(4)$

For we $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ ... $p \equiv 3(4)$ and $q \equiv 3(4)$.

proof we need to fo
llowing quantity. For ~~odd~~ $a,b \in \mathbb{N}$, $a,b>1$, $a \neq b$ and
$(a,b)=1$ we define $S(a,b) := \sum_{i=1}^{\frac{a-1}{2}} \left\lfloor \frac{ib}{a} \right\rfloor$.

Lemma 1 $S(a,b)+S(b,a)=\frac{a-1}{2}\cdot\frac{b-1}{2}=\frac{(a-1)(b-1)}{4}$.

Proof. $S(a,b)=\left|\{(x,y)\in\mathbb{N}^2 \mid 1\le x\le\frac{a-1}{2} \text{ and } y\le x\frac{b}{a}\}\right|$. ($\Leftrightarrow <$ as $(a,b)=1$.)

A

$\frac{(a-1)(b-1)}{4}=\left|\{(x,y)\in\mathbb{N}^2 \mid 1\le x\le\frac{a-1}{2} \text{ and } 1\le y\le\frac{b-1}{2}\}\right|$

C

$y\le x\frac{b}{a}\le\frac{a-1}{2}\frac{b}{a}=\frac{b-\frac{b}{a}}{2}\Rightarrow y\le\left\lfloor\frac{b-\frac{b}{a}}{2}\right\rfloor\le\frac{b-1}{2}\rightsquigarrow$ (b is odd)

$\Rightarrow A\subseteq C$. $B:=C\setminus A=\{(x,y)\in\mathbb{N}^2 \mid 1\le x\le\frac{a-1}{2} \text{ and } 1\le y\le\frac{b-1}{2} \text{ and } y>x\frac{b}{a}\}$ $\Leftrightarrow x<y\frac{a}{b}$ ($\Rightarrow x\le\frac{a-1}{2}$)

$=\{(x,y)\in\mathbb{N}^2 \mid 1\le y\le\frac{b-1}{2} \text{ and } x<y\frac{a}{b}\}\Rightarrow |B|=S(b,a)$

$\rightsquigarrow (C=A\dot\cup B)\ |A|+|B|=|C|$, or $S(a,b)+S(b,a)=|C|=\frac{(a-1)(b-1)}{4}$. ☒

Lemma 2 $p>2$ prime, $a\in\mathbb{N}$ odd, $a\not\equiv 0 \pmod p$. Then $\left(\frac{a}{p}\right)=(-1)^{S(p,a)}$.

Proof-1 Recall $m(a)^{\pm}_0$ and $n(a)^{\pm}_0$. We define numbers $r:=\sum_{x\in m(a)^-} x$ and $s:=\sum_{x\in m(a)^+} x$. By the 2nd observ. above: $\frac{p^2-1}{8}=1+2+\cdots+\frac{p-1}{2}\overset{\text{last deg. of rands}}{\underset{x\in m(a)^0}{\equiv\sum}} x=r+|m(a)^+|\,p-s$ ☒.

If $m(a) = (m_k \mid k = 1, 2, \dots, \frac{p-1}{2})$, then

$$ka = p\left\lfloor \frac{ka}{p} \right\rfloor + m_k$$

$\sum$ for $k = 1, 2, \dots, \frac{p-1}{2}$ we get

$$\frac{p^2-1}{8}a = p\,S(p|a) + v + \Delta. \quad \boxed{2}$$

$\boxed{2} - \boxed{1}$:

$$\underbrace{\frac{p^2-1}{8}}_{\in \mathbb{N}}\underbrace{(a-1)}_{\equiv 0 (2)} = p\underbrace{(S(p|a) - |m(a)^+|)}_{\equiv 1 (2)} + \underbrace{2\Delta}_{\equiv 0 (2)}$$

$$\rightsquigarrow S(p|a) \equiv |m(a)^+| \pmod 2 \quad \overset{\text{Gauss's lemma}}{\rightsquigarrow}$$

$$\left(\frac{a}{p}\right) = (-1)^{|m(a)^+|} = (-1)^{S(p|a)}. \qquad \boxtimes$$

Proof of the QRL is now very easy: $p, q > 2$ different primes

$$\Rightarrow (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{4}} \overset{L1}{=} (-1)^{S(p|q)+S(q|p)} = (-1)^{S(p|q)}(-1)^{S(q|p)} \overset{L2}{=}$$

$$\overset{L2}{=} \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) \rightsquigarrow \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right). \qquad \boxtimes$$

Chapter 6: Integer partitions

number theory, combinatorics
math. analysis, algebra.

For $n \in \mathbb{N}$, a composition of n is any tuple $(a_1, a_2, \dots, a_k) \in \mathbb{N}^k$

s.t. $a_1+a_2+\dots+a_k=n$. How many of them? $c(n)=$ # of c-s of n, $c_k(n)=$ # of c-s of n with exactly k parts.

Example $n=4$: $(1,1,1,1)$, $(1,1,2)$, $(1,2,1)$, $(2,1,1)$, $(2,2)$, $(3,1)$, $(1,3)$ and (4) are 8 compositions of $n=4$. We see that $c_1(4)=1$, $c_2(4)=3$, $c_3(4)=3$, $c_4(4)=1$.

Proposition $n\in\mathbb{N}$, $k\in[n]=\{1,2,\dots,n\}$. Then

$$\boxed{c_k(n)=\binom{n-1}{k-1}}.$$

Consequently,

$$c(n)=\sum_{k=1}^{n} c_k(n)=\sum_{k=1}^{n}\binom{n-1}{k-1}=\sum_{j=0}^{n-1}1^j 1^{n-1-j}\binom{n-1}{j}=(1+1)^{n-1}=$$

$$=2^{n-1}.$$

Proof. 1) Combinatorially: $n=7$, $k=3$: ○○○○○○○

composition → ○ ○|○ ○ ○ ○|○ = $(2,4,1)$ of 7.

2) Algebraically, by GF: $\sum_{n=0}^{\infty} c_k(n)x^n \equiv (x+x^2+x^3+\dots)^k =$

$$=\left(\frac{x}{1-x}\right)^k = x^k(1-x)^{-k}=x^k\sum_{n=0}^{\infty}\binom{-k}{n}(-1)^n x^n.$$ Thus

$$c_k(n)=\binom{-k}{n}(-1)^n=\frac{(-k)(-k-1)\cdots(-k-n+1)}{n!}(-1)^n=$$

$$=\frac{(k+n-1)\cdots k}{n!}=\binom{k+n-1}{n}.$$ Again,

$$c_k(n)=\binom{-k}{n-k}(-1)^{n-k}=\frac{(-k)(-k-1)\cdots(-n+1)}{(n-k)!}(-1)^{n-k}=$$

$$=\frac{(n-1)(n-2)\cdots k}{(n-k)!}=\binom{n-1}{n-k}=\binom{n-1}{k-1}.$$ ☒

Thank you!!!