Directed Graphs Defined by Arithmetic (mod n)

EZRA BROWN
Department of Mathematics
Virginia Tech
Blacksburg, Virginia 24061–0123, USA

1. Introduction. Let a and $n > 0$ be integers, and define $G(a,n)$ to be the directed graph with vertex set $V = \{0,1,\dots,n-1\}$ such that there is an arc from x to y if and only if $y \equiv ax \ (\bmod\ n)$. Recently, Ehrlich [**1**] studied these graphs in the special case $a = 2$ and n odd. He proved that if n is odd, then the number of cycles in $G(2,n)$ is odd or even according as 2 is or is not a quadratic residue mod n. The aim of this paper is to give the analogous results for all a and all positive n. In particular, we show that if a and n are relatively prime, and n is odd, then the number of cycles in $G(a,n)$ is odd or even according as a is or is not a quadratic residue mod n.

Define $GP(a,n)$ be the directed graph with vertex set $V = \{0,1,\dots,n-1\}$ such that there is an arc from x to y if and only if $y \equiv x^a \ (\bmod\ n)$. We determine the number of cycles in $GP(a,n)$ for n a prime power.

2. Preliminary Results. We require a few lemmas. In what follows, write $d|n$ to mean that d is a divisor of n, and let (x,y) and $[x,y]$ denote the greatest common divisor (GCD) and least common multiple (LCM), respectively, of x and y. If $(a,m) = 1$, then (a/m) denotes the familiar Legendre–Jacobi quadratic residue symbol. Finally, let $U_n = \{x : 1 \le x \le n \text{ and } (x,n) = 1\}$, let $\varphi(n)$ denote the Euler phi–function, and if $(a,n) = 1$, then let $ord_n(a)$ be the least positive integer r such that $a^r \equiv 1 \pmod n$.

Lemma 1. *Let $(a,n) = 1$. If $(x_1,x_2,\dots,x_r)$ is a cycle in $G(a,n)$, then (n,x_i) is the same for each i, $1 \le i \le r$.*

Proof. Let $(x_1,x_2,\dots,x_r)$ be a cycle in $G(a,n)$. Since $(a,n) = 1$, it follows that $(n,x_2) = (n,ax_1) = (n,x_1) = 1$, and so for each i, $(n,x_i) = (n,x_1)$ by induction. [We shall call this common value of (n,x_i) the GCD of the cycle $(x_1,x_2,\dots,x_r)$.]

For arbitrary a and n, let $C(a,n)$ denote the number of cycles in $G(a,n)$, and let $c(a,n,d)$ be the number of cycles in $G(a,n)$ with GCD d.

Lemma 2. *Let $(a,n) = 1$. Then* $c(a,n,1) = \dfrac{\varphi(n)}{ord_n(a)}$.

For example, let $a = 3$ and $n = 65$. Then $\varphi(65) = 48$, $ord_5(3) = 4$, $ord_{13}(3) = 3$ and so $ord_{65}(3) = 12$. Thus, $c(3,65,1) = 48/12 = 4$, and the four relevant cycles are

$$(1,3,9,27,16,48,14,42,61,53,29,22),$$
$$(2,6,18,54,32,31,28,19,57,41,58,44),$$
$$(4,12,36,43,64,62,56,38,49,17,51,23), \quad \text{and}$$
$$(7,21,63,59,47,11,33,34,37,46,8,24).$$

Proof. Let $r = ord_n(a)$. Then the elements of the cycle $(1,a,\dots,a^{r-1})$ form a subgroup $< a >$ of U_n of order r. The claim is that the cosets of $< a >$ in U_n and the cycles in $G(a,n)$ with GCD 1 are in one–to–one correspondence. For, writing $x \sim y$ to mean that x and y are in the same coset of $< a >$ in U_n, we see that $x \sim y$ if and only if $x^{-1}y \equiv a^i \pmod{n}$, for some integer i. But this is precisely the condition that x and y lie on a cycle in $G(a,n)$. Hence, $c(a,n,1)$ is equal to the number of cosets of $< a >$ in U_n, i.e. the index of $< a >$ in U_n. But since the group U_n has order $\varphi(n)$, this index is just $\dfrac{\varphi(n)}{ord_n(a)}$.

Lemma 3. *If* $(a,n) = 1$*, and* $d|n$*, then* $c(a,n,d) = c(a, \frac{n}{d}, 1)$*.*

For example, the cycles in $G(2,45)$ with GCD 3 are $(3,6,12,24)$ and $(21,42,39,33)$; the corresponding cycles in $G(2,15)$ with GCD 1 are $(1,2,4,8)$ and $(7,14,13,11)$.

Proof. Let $(x_1, x_2, \ldots, x_r)$ be a cycle in $G(a,n)$ with GCD d. Then $x_2 \equiv ax_1, \ldots, x_r \equiv a^{r-1}x_1$ and $x_1 \equiv a^r x_1 \pmod{n}$ with r positive and minimal. This is true if and only if $(1, a, \ldots, a^{r-1})$ is a cycle in $G(a, \frac{n}{(n,x_1)}) = G(a, \frac{n}{d})$ (clearly with GCD 1). Hence, each cycle in $G(a,n)$ with GCD d has length $r = ord_{n/d}(a)$. Furthermore, x and y lie on a cycle in $G(a,n)$ with GCD d if and only if $y \equiv xa^i \pmod{n}$, i.e. $\frac{y}{d} \equiv \frac{x}{d}a^i \pmod{\frac{n}{d}}$ — which is precisely the condition that $\frac{x}{d}$ and $\frac{y}{d}$ lie on a cycle in $G(a, \frac{n}{d})$. Hence the number of cycles in $G(a,n)$ with GCD d is the same as the number of cycles in $G(a, \frac{n}{d})$ with GCD 1. That is, $c(a,n,d) = c(a, \frac{n}{d}, 1)$.

We are now ready for the main result of this section.

THEOREM A. *If* $(a,n) = 1$*, then*

$$C(a,n) = \sum_{d|n} \frac{\varphi(d)}{ord_d(a)}.$$

Thus,

$$\begin{aligned} C(5,77) &= \frac{\varphi(1)}{ord_1(5)} + \frac{\varphi(7)}{ord_7(5)} + \frac{\varphi(11)}{ord_{11}(5)} + \frac{\varphi(77)}{ord_{77}(5)} \\ &= \frac{1}{1} + \frac{6}{6} + \frac{10}{5} + \frac{60}{30} = 1 + 1 + 2 + 2 = 6. \end{aligned}$$

Proof. For,

$$\begin{aligned} C(a,n) &= \sum_{d|n} c(a,n,d) \\ &= \sum_{d|n} c(a, \frac{n}{d}, 1) \quad \text{(by Lemma 3)} \\ &= \sum_{d|n} c(a,d,1) \qquad \text{(by reordering the sum)} \\ &= \sum_{d|n} \frac{\varphi(d)}{ord_d(a)} \qquad \text{(by Lemma 2).} \end{aligned}$$

3. The parity of $C(a,n)$ for $(a,n)=1$. Next, we determine the parity of the number of cycles in $G(a,n)$ with GCD 1; from that, we determine the parity of $C(a,n)$ for $(a,n)=1$.

Lemma 4. *Let p be an odd prime, let r be a positive integer and let $(a,p)=1$. Put $p-1=2^s q$, where q is odd. (a) If $(a/p)=1$, then $ord_{p^r}(a)|2^{s-1}qp^{r-1}$. (b) If $(a/p)=-1$, then $2^s|ord_{p^r}(a)$.*

Proof. Euler's criterion for the Legendre symbol states that $(a/p)\equiv a^{(p-1)/2}$ (mod p). Thus, if $p-1=2^s q$, where q is odd, then $(a/p)\equiv a^{2^{s-1}q}$ (mod p). We have two cases:

(a) If $(a/p)=1$, then $a^{2^{s-1}q}\equiv 1$ (mod p), so that $ord_p(a)|2^{s-1}q$. If the statement is true for some $r\geq 1$, then $a^{2^{s-1}qp^{r-1}}=1+kp^r$; raising both sides to the pth power, we have $a^{2^{s-1}qp^r}=(1+kp^r)^p\equiv 1$ (mod p^{r+1}). Hence, $ord_{p^r}(a)|2^{s-1}qp^{r-1}$ by induction.

(b) If $(a/p)=-1$, then $a^{2^{s-1}q}\equiv -1$ (mod p), so that $2^s|ord_p(a)$. Since $ord_p(a)$ is a divisor of $ord_{p^r}(a)$ for $r\geq 1$, we are done.

Lemma 5. *Let $(a,n)=1$ with n odd. If $n=p^r$, where p is a prime and if $(a/p)=-1$, then $c(a,n,1)$ is odd; in all other cases, $c(a,n,1)$ is even.*

Proof. Let $p-1=2^s q$, where q is odd. By Lemma 4, if $(a/p)=-1$, then $ord_{p^r}(a)=2^s k$ with k odd. Since $\varphi(p^r)=p^{r-1}(p-1)=p^{r-1}2^s q$, it follows from Lemma 2 that

$$c(a,p^r,1)=\frac{\varphi(p^r)}{ord_{p^r}(a)}=\frac{p^{r-1}q}{k},$$

which is an odd number. Hence $c(a,p^r,1)$ is odd.

We must now show that in all other cases, $c(a,n,1)$ is even.

First, if $n=p^r$ with p as above, and if $(a/p)=1$, then the highest power of 2 dividing $ord_{p^r}(a)$ is 2^{s-1}. Since $2^s|\varphi(p^r)$, it follows that the fraction $\frac{\varphi(p^r)}{ord_{p^r}(a)}$ is even.

Next, if $n=\prod_{i=1}^g p_i^{e_i}$ with $g>1$ and $p_i-1=2^{s_i}q_i$, then

$$ord_n(a)\,|\,\left[p_1^{e_1-1}\cdot 2^{s_1}q_1,\dots,p_g^{e_g-1}\cdot 2^{s_g}q_g\right]=\prod_{i=1}^g p_i^{e_i-1}\left[q_1,\dots,q_g\right]\cdot 2^M,$$

where $M=\max(s_1,\dots,s_g)$. Now let $S=\sum_{i=1}^g s_i$. Since n is divisible by at least two distinct odd primes, it follows that $S>M$, so that $c(a,n,1)=\dfrac{\varphi(n)}{ord_n(a)}$ is divisible by 2^{S-M}. Hence, $c(a,n,1)$ is even.

A slight modification of the above proof yields the following:

Lemma 6. *Let $(a,n)=1$ with n even.*

(a) If n is divisible either by 8 or by more than one odd prime, or if $n=4p^e$ with p an odd prime, then $c(a,n,1)$ is even.

(b) If p is an odd prime, then $c(a,p^e,1)=c(a,2p^e,1)$.

(c) $c(a,1,1)=c(a,2,1)=1$ and $c(a,4,1)=\dfrac{(-1/a)+3}{2}$.

We may now prove our main results.

THEOREM B. *Let a and n be relatively prime, and let n be odd. Then the number of cycles in $G(a,n)$ is odd or even according as a is or is not a quadratic residue mod n. That is,* $C(a,n) \equiv \dfrac{1+(a/n)}{2}$ *(mod 2).*

For example, $C(3,1001)$ is even because $(3/1001) = (1001/3) = (2/3) = -1$. A bit of direct calculation reveals that $ord_7(3) = 6, ord_{11}(3) = 5$ and $ord_{13}(3) = 3$, so that

$$\begin{aligned} C(3,1001) &= \sum_{d|1001} \frac{\varphi(d)}{ord_d(a)} \\ &= 1 + \frac{6}{6} + \frac{10}{5} + \frac{12}{3} + \frac{60}{30} + \frac{72}{6} + \frac{120}{15} + \frac{720}{30} \\ &= 1+1+2+4+2+12+8+24 = 54, \end{aligned}$$

which is indeed even. Somewhat more tricky is the evaluation of $C(2159, pq)$, where $p = 205909401806482731234 5603$ and $q = 534286141271831814831333517$ are both primes. However, since $pq \equiv 3 \pmod 4$, we see that $(2159/pq) = -(pq/2159) = -(743/2159) = (2159/743)$, which reduces to the product $(2/673)(8/35)$, or -1. Hence $C(2159, pq)$ is even.

Proof. Let $n = \prod_{i=1}^{g} p_i^{e_i}$ with each p_i odd, and suppose $(a,n) = 1$. It follows from Theorem A and Lemma 5 that

$$C(a,n) = \sum_{d|n} \frac{\varphi(d)}{ord_d(a)} \equiv 1 + \sum_{i=1}^{g} \sum_{j=1}^{e_i} \frac{\varphi(p_i^j)}{ord_{p_i^j}(a)} \pmod 2,$$

since all other terms are even. If we order the primes p_i so that for some integer f (which might be 0), $(a/p_i) = 1$ if and only if $i > f$, then we see that

$$\begin{aligned} C(a,n) &\equiv 1 + \sum_{i \le f} \sum_{j=1}^{e_i} 1 \pmod 2 \\ &\equiv 1 + \sum_{i \le f} e_i \pmod 2. \end{aligned}$$

On the other hand, since n is odd and $(a,n) = 1$, we use the well–known properties of the Legendre and Jacobi symbols to see that

$$\begin{aligned} (a/n) &= \prod_{i=1}^{g} (a/p_i)^{e_i} \\ &= \prod_{i \le f} (-1)^{e_i} \qquad \text{(since } (a/p_i) = 1 \text{ for } i > f\text{)} \\ &= (-1)^{\sum_{i \le f} e_i}, \qquad \text{so that} \\ (-1)^{C(a,n)} &\equiv (-1)^{1+\sum_{i \le f} e_i} \equiv -(a/n) \pmod 2. \end{aligned}$$

Hence $C(a,n)$ is odd if $(a/n) = 1$, and $C(a,n)$ is even if $(a/n) = -1$, and we are done.

THEOREM C. *Let a and n be relatively prime, let n be even, and write $n = 2^e n'$, where n' is odd.*

(a) If $e = 1$, then $G(a, n)$ has an even number of cycles.

(b) If $e \geq 2$, then the number of cycles in $G(a, n)$ is even or odd according as -1 is or is not a quadratic residue mod n'. That is,

$$C(a, n) \equiv \frac{1 - (-1/n')}{2} \ (\ mod\ 2).$$

Proof. Theorem C follows from Theorem A and Lemma 6 in the same way thatTheorem B follows from Theorem A and Lemma 5.

4. The parity of $C(a, n)$ for arbitrary a and n. We are now ready to extend Theorems B and C to the graphs $G(a, n)$, where a and n are not relatively prime. The principal observation is the correspondence between the cycles in $G(a, qm)$ and the cycles in $G(a, m)$. Specifically, we have the following:

Lemma 7. *Suppose $(m, a) = 1$ and suppose that each prime divisor of q divides a. Then $C(a, qm) = C(a, m)$.*

Proof. Let x be an integer mod qm. We may write $x = (x_a, y)$, where $(y, a) = 1$ and each prime divisor of x_a divides a. Thus, $(x_a, q) = 1$. Now let $i \geq 0$ and $r > 0$ be minimal and satisfy

$$a^{i+r} x \equiv a^i x \,(\text{mod } qm).$$

This happens if and only if $y(a^r - 1)(a^i x_a) \equiv 0 \,(\text{mod } qm)$. But $(a^i x_a, q) = 1$, and $(y(a^r - 1), m) = 1$. Hence, the above congruence holds if and only if

$$q | y(a^r - 1) \qquad \text{and} \qquad m | a^i x_a.$$

Thus, $(a^i x, \ldots, a^{i+r-1} x)$ is a cycle in $G(a, qm)$ if and only if i is the least nonnegative integer such that $m | a^i x$ and $(y, ay, \ldots, a^{r-1} y)$ is a cycle in $G(a, q)$, where y is the largest divisor of x relatively prime to m. But this means that the cycles of $G(a, qm)$ and the cycles of $G(a, q)$ are in one–to–one correspondence, i.e. $C(a, qm) = C(a, m)$.

As a direct consequence of Lemma 7, we have the following result:

THEOREM D. *If a and n are positive integers, then the parity of $C(a, n)$ is equal to the parity of $C(a, n')$, where n' is the largest divisor of n that is relatively prime to a.*

5. The cycle structure of the graphs $GP(a, n)$ for n a prime. Let $GP(a, n)$ be the directed graph with vertex set $V = \{0, 1, \ldots, n-1\}$ such that there is an arc from x to y if and only if $y \equiv x^a$ (mod n). Let $CP(a, n)$ denote the number of cycles in the graph $GP(a, n)$.

There are some interesting differences between the graphs $GP(a, n)$ and $G(a, n)$. For example, if $(a, n) = 1$, then every vertex of $G(a, n)$ lies on a cycle. This is not the case for the vertices of $GP(a, n)$. If p^n is a prime power, then $GP(a, p^n)$ looks like a union of charm bracelets, with each charm a tree that corresponds to a coset of a certain subgroup U of roots of unity mod p^n. In particular, if we write $\varphi(p^n) = qr$, where $(q, a) = 1$, every prime divisor of r divides a, and m is the least positive integer such that $r | a^m$, then U consists of the a^mth roots of unity mod $\varphi(p^n)$.

Our principal result of this section is the following theorem:

THEOREM P. *If p^n is an odd prime, then there is a one–to–one correspondence between the cycles of $GP(a,p^n)$ and the cycles of $G(a,q)$, where q is the largest divisor of $\varphi(p^n)$ that is relatively prime to a. Furthermore,*

$$CP(a,p^n) = 1 + \sum_{d|\varphi(p^n),\,(d,a)=1} \frac{\varphi(d)}{ord_d(a)}.$$

The following lemma leads us to the proof of Theorem P.

Lemma 8. *Let p^n be a prime power; let g be a primitive root (mod p); let $(a,p)=1$ and write $\varphi(p^n)=qr$, where $(q,a)=1$ and every prime divisor of r divides a. Then x and y lie on a cycle in $GP(a,p^n)$ if and only if either (a) there exist integers j and k such that $x \equiv g^{rj}$ (mod p^n), $y \equiv g^{rk}$ (mod p), and j and k lie on a cycle of $G(a,q)$, or (b) $x=y=0$.*

Proof. If $p|x$, then for some positive integer s, $x^{a^s} \equiv 0 \pmod{p^n}$. Thus, if $p|x$, then x lies on a cycle in $GP(a,p^n)$ if and only if $x \equiv 0 \pmod{p^n}$. From here on, we assume that x and y are relatively prime to p.

If x is a vertex of $GP(a,p^n)$, then we may write $x \equiv g^t \pmod{p^n}$ for some integer t with $0 \le t < \varphi(p^n)$. Let us first show that x lies on a cycle of $GP(a,p^n)$ if and only if $r|t$. We have the following sequence of equivalent statements:

$$\begin{array}{ll} & x \text{ lies on a cycle of } GP(a,p^n) \\ \text{if and only if} & x^{a^s} \equiv x \pmod{p^n} \text{ for some positive integer } s \\ \text{if and only if} & g^{t(a^s-1)} \equiv 1 \pmod{p^n} \text{ for some positive integer } s \\ \text{if and only if} & \varphi(p^n)|t(a^s-1). \end{array}$$

Hence, if x lies on a cycle of $GP(a,p^n)$, then $rq|t(a^s-1)$. Now each prime divisor of r divides a, so it follows that $(r, a^s-1)=1$. We conclude that $r|t$.

Conversely, suppose that $r|t$, so that $x \equiv g^{rj} \pmod{p^n}$ for some integer j. If $j=0$, then $x=1$, which is clearly on its own cycle; since $g^{\varphi(p^n)} \equiv 1 \pmod{p^n}$, we may assume that $1 \le j \le q-1$. The above argument shows that x is on a cycle if and only if $rq|rj(a^s-1)$ for some integer s. Since $1 \le j \le q-1$, it follows that $q|(a^s-1)$. In particular, if $s = ord_q(a)$, then we may conclude that x lies on a cycle of length s.

Next, x and y will lie on a common cycle if and only if $x \equiv g^{rj} \pmod{p^n}$ and $y \equiv g^{rk} \pmod{p^n}$ lie on a common cycle of $GP(a,p^n)$. It is straightforward to verify that this happens if and only if there exists an integer m such that $ja^m \equiv k \pmod{q}$ — i.e., that j and k lie on a cycle of $G(a,q)$.

Finally, if

$$(j, ja, \ldots, k \equiv ja^m, \ldots, ja^{s-1})$$

is a cycle in $G(a,q)$, then it follows that $s = ord_q(a)$, which means that

$$(g^{rj}, g^{rja}, \ldots, g^{rja^m}, \ldots, g^{rja^{s-1}})$$

is a cycle in $PG(a,p^n)$, and we are done.

Theorem P now follows from Lemma 8 and Theorem A, and from the fact that there is one extra cycle in $PG(a,p^n)$ — the cycle consisting of the directed loop from the vertex 0 to itself.

REFERENCE

[**1.**] Amos Ehrlich, Cycles in doubling diagrams mod m, *Fibonacci Quarterly* **32** (1994), 74–78.

AMS Classification Numbers: 11A07, 05D20, 11A15