

involve

a journal of mathematics

Finding cycles in the k -th power digraphs
over the integers modulo a prime

Greg Dresden and Wenda Tu



Finding cycles in the k -th power digraphs over the integers modulo a prime

Greg Dresden and Wenda Tu

(Communicated by Kenneth S. Berenhaut)

For p prime and $k \geq 2$, let us define $G_p^{(k)}$ to be the digraph whose set of vertices is $\{0, 1, 2, \dots, p-1\}$ such that there is a directed edge from a vertex a to a vertex b if $a^k \equiv b \pmod{p}$. We find a new way to decide if there is a cycle of a given length in a given graph $G_p^{(k)}$.

Introduction

Let $k \geq 2$ be an integer and let p be prime. Let us define $G_p^{(k)}$ to be the digraph whose set of vertices is $\{0, 1, 2, \dots, p-1\}$ such that there is a directed edge from a vertex a to a vertex b if $a^k \equiv b \pmod{p}$.

This paper extends the results given in [Sommer and Křížek 2004] (which provides a way to determine whether there is a cycle of length t in a given graph $G_p^{(2)}$) and [Wilson 1998] (which considers $G_p^{(k)}$; see also [Sommer and Křížek 2009]). In this paper, we provide our own way to determine the existence of a cycle of given length in $G_p^{(k)}$. First, we examine the existence of length- t cycles where t is prime. Later on, we explore the case of cycles of length u where u is composite, and we conclude with a study of digraphs that admit some cycle lengths but do not allow others.

Now, we will introduce one of the key theorems of this paper, mentioned in [Niven, Zuckerman and Montgomery 1991]. Here, ϕ stands for the Euler totient function.

Theorem 1. *Suppose $m = 1, 2, 4, p^\alpha$ or $2p^\alpha$, where p is an odd prime and α is a positive integer. If $\gcd(a, m) = 1$ then the congruence $x^n \equiv a \pmod{m}$ has $\gcd(n, \phi(m))$ solutions or no solution, according to whether*

$$a^{\phi(m)/\gcd(n, \phi(m))} \equiv 1 \pmod{m}$$

or not.

MSC2010: primary 05C20; secondary 11R04.

Keywords: digraphs, cycles, graph theory, number theory.

**On the existence of length- t cycles given t prime,
and length- u cycles given $u \geq 2$**

Based on the theorem in our Introduction, we have the following corollaries, which are crucial in determining the existence of a length- t cycle for t prime.

Corollary 2. *Let p be a prime. The congruence $x^n \equiv 1 \pmod p$ has $\gcd(n, p - 1)$ solutions.*

Corollary 3. *Let p be a prime and let $k \geq 2$. The subgraph $G_p^{(k)} \setminus \{0\}$ has $\gcd(k - 1, p - 1)$ cycles of length 1.*

Since we are curious about the existence of length- t cycles in $G_p^{(k)}$ given t prime, we want to know if the following equations have any solutions:

$$x^{k^t} \equiv x \pmod p, \quad x^k \not\equiv x \pmod p.$$

By our two corollaries, the above equations are equivalent to

$$\gcd(k^t - 1, p - 1) > \gcd(k - 1, p - 1).$$

Similarly, since we are also curious about the existence of length- u cycles in $G_p^{(k)}$ given u composite, we want to know if the following equations have any solutions (here, u_i runs over the proper divisors of u):

$$x^{k^u} \equiv x \pmod p, \quad x^{k^{u_1}} \not\equiv x \pmod p, \quad x^{k^{u_2}} \not\equiv x \pmod p, \quad \dots$$

Once again, our corollaries tell us that the above equations are equivalent to

$$\gcd(k^u - 1, p - 1) > \gcd(k^{u_i} - 1, p - 1)$$

for u_i running over all proper divisors of u . So, we have the following results:

Theorem 4. *Given $u \geq 2$, $k \geq 2$, and p prime, there exists a length- u cycle in $G_p^{(k)}$ if and only if $\gcd(k^u - 1, p - 1) > \gcd(k^{u'} - 1, p - 1)$ for all proper divisors u' of u .*

Remark. Theorem 4 follows from Theorem 5.6 of [Somer and Křížek 2009], which also gives formulas for how many cycles exist of a given length; if t is prime, for example, then the number of length- t cycles is

$$\frac{\gcd(k^t - 1, p - 1) - \gcd(k - 1, p - 1)}{t}.$$

The following theorem, which is a result of [Lucheta, Miller and Reiter 1996, pp. 230–231], is also a special case of a more general result in [Wilson 1998, pp. 232–233]. Another version with $k = 2$ appeared in [Somer and Křížek 2004, Theorem 3.3].

Theorem 5 (Lucheta, Miller, Reiter). *Let p be a prime. There exists a cycle of length u in $G_p^{(k)}$ if and only if $u = \text{ord}_d k$ for some divisor d of $p - 1$ with $\gcd(d, k) = 1$, where $\text{ord}_d k$ denotes the multiplicative order of k modulo d .*

Here are four corollaries following from Theorems 4 and 5 that give us precise information on what cycle lengths are possible (or impossible) in $G_p^{(k)}$ for various primes p and powers k :

Corollary 6. *Fix a prime t . Given any integer $k \geq 2$, there are infinitely many primes p such that $G_p^{(k)}$ has a length- t cycle. Moreover, $G_p^{(k)}$ contains a 1-cycle for all primes p .*

Corollary 7. *Fix an integer $u \geq 2$. Given any integer $k \geq 2$, there are infinitely many primes p such that $G_p^{(k)}$ does not have a length- u cycle.*

Corollary 8. *Fix an integer $u \geq 2$. Let $p = 2^{2^n} + 1$ be a Fermat prime, where $n \geq 0$. The possible cycle lengths in $G_p^{(k)}$ for p a Fermat prime are very limited:*

- (1) *There are never any odd-length cycles (aside from the length-1 cycles).*
- (2) *If k is even, there are no cycles at all (aside from the length-1 cycles) in $G_p^{(k)}$.*
- (3) *If k is odd and u is even, $G_p^{(k)}$ contains a length- u cycle if and only if $u \mid \text{ord}_{p-1} k$. Moreover, $\text{ord}_{p-1} k \mid 2^{2^n - 2}$ if $n \geq 2$ and $\text{ord}_{p-1} k \mid 2^{2^n - 1}$ if $n = 0$ or 1 .*

Corollary 9. *Fix an integer $u \geq 2$, and let p be prime. Then, there are infinitely many integers k such that $G_p^{(k)}$ contains no length- u cycle.*

Proof of Corollary 6. Since $\gcd(1, \sum_{i=0}^{t-1} k^i) = 1$, by Dirichlet's theorem on the infinitude of primes in arithmetic progressions we know that there are infinitely many primes p such that $p \equiv 1 \pmod{\sum_{i=0}^{t-1} k^i}$. Now given such a prime p , we have

$$\gcd\left((k-1) \sum_{i=0}^{t-1} k^i, p-1\right) \geq \sum_{i=0}^{t-1} k^i \quad \text{or} \quad \gcd(k^t - 1, p-1) \geq \sum_{i=0}^{t-1} k^i.$$

On the other hand, $\gcd(k-1, p-1) \leq k-1$. Since it is not hard to see that $k-1 < \sum_{i=0}^{t-1} k^i$, we have $\gcd(k^t - 1, p-1) > \gcd(k-1, p-1)$. Thus, by Theorem 4, we can conclude that there are infinitely many primes p such that $G_p^{(k)}$ has a length- t cycle, as desired. Finally, the last assertion of our statement holds, since both 0 and 1 are clearly vertices in 1-cycles. \square

Proof of Corollary 7. Let q_1, q_2, \dots be the odd primes in order of size, and let q_r be the largest prime less than or equal to k^u ; since both u and k are at least 2, then q_r is at least 3. By the Chinese remainder theorem and Dirichlet's theorem, there exist infinitely many primes p such that

$$p \equiv 3 \pmod{4}, \quad p \equiv 2 \pmod{q_1 q_2 \cdots q_r}.$$

The first equivalence implies $2 \mid p-1$ but $4 \nmid p-1$, while the second implies $p-1$ is relatively prime to $q_1 q_2 \cdots q_r$. Now suppose $G_p^{(k)}$ actually does have a length- u cycle for $u \geq 2$. It follows from Theorem 5 that $u = \text{ord}_d k$ for some divisor $d > 1$

of $p - 1$ (note that if $d = 1$ then this would imply $u = 1$, a contradiction), with d relatively prime to k . Let us consider the options, keeping in mind what we just wrote about $p - 1$. If k is odd, then either $d = 2$ or $d \geq q_{r+1}$. But if $d = 2$ then $u = \text{ord}_2 k = 1$, which is a contradiction. Hence, our only option is $d \geq q_{r+1}$. If k is even, then d must be odd and so again our only option is $d \geq q_{r+1}$. But with $d \geq q_{r+1}$, since $1 < k^u < q_{r+1}$ we have u is not, in fact, the order of $k \bmod d$, which contradicts our statement earlier that $u = \text{ord}_d k$. Hence, $G_p^{(k)}$ does not have a length- u cycle for $u \geq 2$. \square

Before we move on to the next proof, we need to establish this useful result.

Lemma 10. *For k odd and $a \geq 2$, the order $\text{ord}_{2^{a+1}} k$ is either equal to $\text{ord}_{2^a} k$ or to $2 \text{ord}_{2^a} k$.*

Proof of Lemma 10. If we let $w = \text{ord}_{2^a} k$, then we know that $2^a \mid k^w - 1$. Consider $k^{2w} - 1 = (k^w - 1)(k^w + 1)$. We know 2^a divides $k^w - 1$ and since k is odd, 2 divides $k^w + 1$, so we know 2^{a+1} divides $k^{2w} - 1$. Hence, $\text{ord}_{2^{a+1}} k$ divides $2w$, but $\text{ord}_{2^{a+1}} k$ is at least w , and so we conclude that $\text{ord}_{2^{a+1}} k$ is either w or $2w$, as desired. \square

We are now ready for the following:

Proof of Corollary 8. Let p be the Fermat prime $2^{2^n} + 1$ where $n \geq 0$, so $p - 1 = 2^{2^n}$. Now, suppose $G_p^{(k)}$ contains a cycle of length $u \geq 2$. Then by Theorem 5, $u = \text{ord}_d k$ for some divisor d of $p - 1 = 2^{2^n}$. By Euler's generalization of Fermat's little theorem, this implies $u \mid \phi(d)$, but d is a power of 2 and so (thanks to the well-known formulas for Euler's phi function) this implies u is as well. By Theorem 5, we also have d and k are relatively prime; since $u \mid d$, we know u and k are relatively prime as well. With this in mind, let us consider the possibilities for u and k . We cannot have $u \geq 2$ be an odd integer, as this contradicts $u \geq 2$ being a power of 2; hence, $G_p^{(k)}$ never contains a cycle of length $u \geq 2$ for u odd. We also cannot have u and k both be even integers, as this contradicts u and k being relatively prime; hence, $G_p^{(k)}$ contains no cycles of length u for u and k both even.

The only option left is to have $u \geq 2$ even and $k \geq 2$ odd. Theorem 5 tells us that we have a length- u cycle if and only if $u = \text{ord}_d k$ for some divisor d of $p - 1$; let us establish that this is equivalent to $u \mid \text{ord}_{p-1} k$. For the first Fermat prime $p = 2^{2^0} + 1 = 3$, it is easy to verify that there are no even-length cycles in $G_3^{(k)}$ because this graph contains only the vertices $\{0, 1, 2\}$; likewise, $\text{ord}_{p-1} k = 1$ and this admits no even divisors. For the next Fermat prime $p = 2^{2^1} + 1 = 5$, similar calculations reveal that we can have even length- u cycles only for $k \equiv 3 \pmod{4}$ and for $u = 2$, in which case u is indeed an even divisor of $2 = \text{ord}_{p-1} k$ (and vice versa). For both of those two cases (namely, for $p = 2^{2^n} + 1$ with $n = 0$ or 1), it is easy to check that $\text{ord}_{p-1} k \mid 2^{2^n - 1}$, as desired.

It remains to consider the other Fermat primes $p = 2^{2^n} + 1$ for $n \geq 2$. If $u = \text{ord}_d k$ for some divisor d of $p - 1 = 2^{2^n}$, then (recalling that u and d and $p - 1$ are all

powers of 2) it is certainly true that $u \mid \text{ord}_{p-1} k$, as $\text{ord}_d k$ cannot be greater than $\text{ord}_{p-1} k$ and both are powers of 2. For the other direction, suppose $u \mid \text{ord}_{p-1} k$, and let us show that $u = \text{ord}_d k$ for some divisor d of $p - 1$. Starting with 1 as the order of $k \pmod 2$, we imagine finding the orders of $k \pmod{2^2}$, $\pmod{2^3}$, $\pmod{2^4}$, and so on, up to $\pmod{2^n}$. Lemma 10 tells us that at each step, the order of k either stays the same or doubles. At the last step in this sequence (modulo 2^{2^n}) the order of k is a multiple of u . Hence, at some step along the way (say, when our modulus is 2^b for $b \leq 2^n$) we know that the order of $k \pmod{2^b}$ is equal to u . Hence, we let $d = 2^b$ and we have $u = \text{ord}_d k$ for d a divisor of $p - 1$, as desired.

Finally, we recall from [Gallian 2010, p. 160] that the multiplicative group of units modulo 2^{2^n} , commonly written $(\mathbb{Z}_{2^{2^n}})^*$, is isomorphic to $\mathbb{Z}_{2^{2^n-2}} \oplus \mathbb{Z}_2$ for $n \geq 2$. Hence, the order of any odd number k modulo $p - 1$ will be a divisor of 2^{2^n-2} , as desired. \square

Proof of Corollary 9. Note that if p is a Fermat prime, then by Corollary 8 we can simply choose k to be any even number. Of course, for $p = 2$ the conclusion is trivial. For the more general case, we choose $k \geq 2$ to be an integer equivalent to $1 \pmod{p - 1}$. There are clearly infinitely many such k . Note that $\text{gcd}(k, p - 1) = 1$ and also $k \equiv 1 \pmod d$ for any divisor d of $p - 1$. Thus, $\text{ord}_d k = 1$ for any divisor d of $p - 1$ and so by Theorem 5 we know $G_p^{(k)}$ has no u -cycles for any $u \geq 2$. \square

On the existence of cycles of different lengths in the same digraph

We now consider cycles of composite length, and we show that the existence of certain cycles implies the existence of other, longer cycles.

Theorem 11. *Let $u = \text{lcm}(u_1, u_2)$, where u_1 and u_2 are positive integers. If $G_p^{(k)}$ contains cycles of length u_1 and length u_2 respectively, then $G_p^{(k)}$ also contains a cycle of length u .*

Proof. Suppose in $G_p^{(k)}$ there exist cycles of lengths u_1 and u_2 . By Theorem 5, we know that there exist d_1 and d_2 such that $d_1 \mid (p - 1)$, $d_2 \mid (p - 1)$ and $u_1 = \text{ord}_{d_1} k$, $u_2 = \text{ord}_{d_2} k$. Also, let $d = \text{lcm}(d_1, d_2)$ and $u = \text{lcm}(u_1, u_2)$. Since $d_1 \mid (k^{u_1} - 1)$ and $u_1 \mid u$, we have $d_1 \mid (k^u - 1)$. By the same reasoning, $d_2 \mid (k^u - 1)$. Therefore, $d \mid (k^u - 1)$; that is, $k^u \equiv 1 \pmod d$. So, $\text{gcd}(d, k) = 1$. Assume there exists $u' \leq u$ such that $k^{u'} \equiv 1 \pmod d$. So, $k^{u'} \equiv 1 \pmod{d_1}$ and $k^{u'} \equiv 1 \pmod{d_2}$. Since u_1 is the order of $k \pmod{d_1}$, we have $u_1 \mid u'$. Likewise, $u_2 \mid u'$. Therefore, $\text{lcm}(u_1, u_2) \mid u'$; that is, $u \mid u'$. So $u \leq u'$. By assumption we know $u' \leq u$; thus, $u = u'$. So, the order of $k \pmod d$ is u . Since $d = \text{lcm}(d_1, d_2)$, we have $d \mid (p - 1)$. Thus again by Theorem 5, we know there is a length- u cycle in $G_p^{(k)}$. \square

Corollary 12. *Let $u = \text{lcm}(u_1, u_2, u_3, \dots, u_n)$, where u_1, u_2, \dots, u_n are positive integers. If $G_p^{(k)}$ contains a cycle of length u_i for each i , then $G_p^{(k)}$ also contains a cycle of length u .*

It turns out that for even k , the opposite direction is not always true. Later we present a digraph $G_p^{(k)}$ that has a 12-cycle and a 1-cycle but no cycles of length 2, 3, 4, or 6. The following result indicates that this is hardly an isolated occurrence.

Theorem 13. *Let u be a composite number and let k be even.*

- (1) *If $k \neq 2$ or $u \neq 6$, then there exist infinitely many primes p such that in $G_p^{(k)}$ there exists a length- u cycle but no length- u' cycles in which $u' \geq 2$ is a positive divisor of u .*
- (2) *For the case $k = 2$ and $u = 6$, suppose for some prime p that $G_p^{(2)}$ has a cycle of length 6. Then there must also exist a cycle of either length 2 or 3 in $G_p^{(2)}$; furthermore, if $G_p^{(2)}$ has cycles of length 6 and 3 then it must also have a cycle of length 2. The smallest prime p such that $G_p^{(2)}$ has both a length-6 and a length-2 cycle is $p = 19$; in this case, though, $G_{19}^{(2)}$ does not have a length-3 cycle. The smallest prime p such that $G_p^{(2)}$ has cycles of lengths 2, 3, and 6 is $p = 43$.*

Before we start our proof, we need to introduce a very useful lemma proved independently by Bang [1886] and Zsigmondy [1892], as seen in a recent paper by Roitman [1997]:

Lemma 14 (Bang and Zsigmondy). *Let k and u be integers greater than 1. There exists a prime divisor q of $k^u - 1$ such that q does not divide $k^j - 1$ for all j where $0 < j < u$, except exactly in the following cases:*

- (1) $k = 2^s - 1$, where $s \geq 2$, and $u = 2$;
- (2) $k = 2$ and $u = 6$.

Proof of Theorem 13. First, let us discuss the case where $k = 2$ and $u = 6$; that is, we suppose there exists a length-6 cycle in $G_p^{(2)}$. By Theorem 4, we must have $\gcd(2^6 - 1, p - 1) > 1$. Now since $2^6 - 1 = 63$, we know $p - 1$ must be divisible by either 7 or 3. Since $2^3 - 1$ is 7 and of course $2^2 - 1$ is 3, we conclude that either $\gcd(2^3 - 1, p - 1) > 1$ or $\gcd(2^2 - 1, p - 1) > 1$ and hence (again by Theorem 4) we must have a cycle of length 3 or length 2. Now suppose (for the sake of argument) that $G_p^{(2)}$ happens to have both a length-6 cycle and a length-3 cycle but no length-2 cycle. If we let A_i represent the number of cycles of length i in the graph of $G_p^{(2)}$, then Theorem 5.6 of [Sommer and Křížek 2009] tells us

$$A_6 = \frac{1}{6}(\gcd(p - 1, 63) - A_1 - 2A_2 - 3A_3).$$

Clearly, $A_1 = 1$ since the only nontrivial solution to $x^2 \equiv x \pmod{p}$ is $x = 1$. We are assuming that $A_2 = 0$ and that A_3 and A_6 are both positive, and so the above equation becomes

$$A_6 = \frac{1}{6}(\gcd(p - 1, 63) - 1 - 3A_3).$$

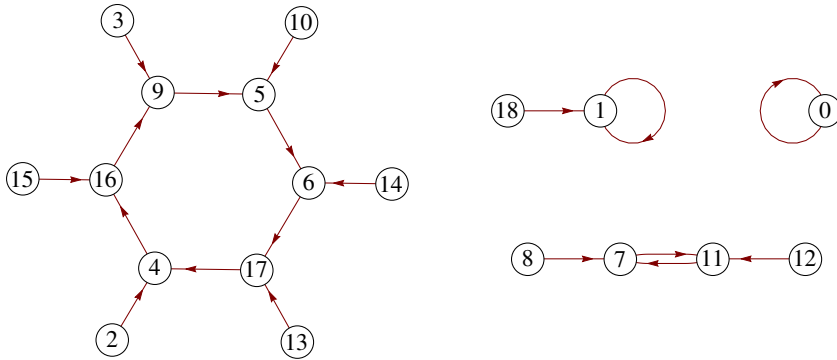


Figure 1. The digraph $G_{19}^{(2)}$ has a 6-cycle and 2-cycle but no 3-cycle.

Since $A_3 > 0$, for A_6 to be a nonzero integer we must have $\gcd(p - 1, 63)$ be either 9, 21, or 63, which are all equivalent to 3 mod 6. But $1 + 3A_3$ will be equivalent to 1 or 4 mod 6, and the difference of these two expressions can never be 0 mod 6, which contradicts A_6 being an integer. Hence, the presence of a length-6 cycle and a length-3 cycle really does force there to be a length-2 cycle.

By inspection, $p = 19$ is the smallest prime p such that $G_p^{(2)}$ has a 6-cycle and a 2-cycle; it is easily seen that it does not have a 3-cycle. Also by inspection, $p = 43$ is the smallest prime p such that $G_p^{(2)}$ has a 6-cycle, a 2-cycle, and a 3-cycle. See Figure 1 for the graph of $G_{19}^{(2)}$.

Now if $k \neq 2$ or $u \neq 6$, then in order to prove the theorem it is sufficient to show that there are infinitely many primes p such that for the graph $G_p^{(k)}$ the following conditions hold: for u_1, u_2, \dots nontrivial proper divisors of u ,

$$\gcd(k^u - 1, p - 1) > 1, \quad \gcd(k^{u_1} - 1, p - 1) = 1, \quad \gcd(k^{u_2} - 1, p - 1) = 1, \quad \dots$$

(By Corollaries 2 and 3, these equations will also imply that the only cycles of length 1 in $G_p^{(k)}$ will be the 1-cycle with vertex 0 and the 1-cycle with vertex 1.) By Lemma 14, we know that there exists a prime divisor $q \mid k^u - 1$ such that $q \nmid k^j - 1$ for $0 < j < u$. Now, consider the set of equivalence relations

$$p - 1 \equiv 0 \pmod q, \tag{1}$$

$$p - 1 \equiv 1 \pmod s, \tag{2}$$

where $s = \text{lcm}(k^{u_1} - 1, k^{u_2} - 1, \dots)$. Since q is prime, it is obvious that $q \nmid s$ and therefore we can apply the Chinese remainder theorem to get

$$p - 1 \equiv q[q^{-1}]_s \pmod{qs},$$

where $[q^{-1}]_s$ is the unique positive integer less than s that is the inverse of q modulo s .

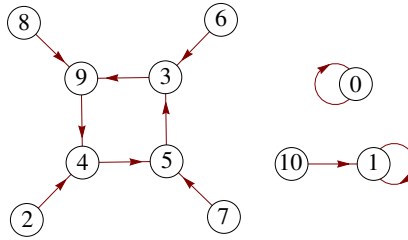


Figure 2. The digraph $G_{11}^{(2)}$ has a 4-cycle but no 2-cycle.

Thus, $p = (q[q^{-1}]_s + 1) + qs \cdot n$, where $n \in \mathbb{N}$. Since $q[q^{-1}]_s \equiv 1 \pmod s$, we know $q[q^{-1}]_s + 1 \equiv 2 \pmod s$, so $\gcd(q[q^{-1}]_s + 1, s) \leq 2$. Now k is even, so s is odd, and we know $\gcd(q[q^{-1}]_s + 1, s) = 1$. On the other hand, it is obvious that $q \nmid q[q^{-1}]_s + 1$; therefore $\gcd(q[q^{-1}]_s + 1, qs) = 1$. Thus, by Dirichlet’s theorem, there are infinitely many primes p of the form $p = (q[q^{-1}]_s + 1) + qs \cdot n$, as desired. \square

Now, let us do some examples to illustrate the methods given above.

Example. For p a prime, $p \equiv 11 \pmod{15}$, we know $G_p^{(2)}$ always has a 4-cycle but never has a 2-cycle. This can be shown via the methods of the above proof with $k = 2$, $u = 4$, and $u_1 = 2$, so $q = 5$ and $s = 3$. The two smallest primes p of this type are 11 and 41. The digraph for $G_{11}^{(2)}$ is given in Figure 2.

Example. Likewise, using $k = 2$, $u = 9$, and $u_1 = 3$, we can show that for p a prime equivalent to $366 \pmod{511}$, the graph $G_p^{(2)}$ always has a 9-cycle but never has a 3-cycle. The smallest prime equivalent to $366 \pmod{511}$ is 877, and a partial digraph for $G_{877}^{(2)}$ is given in Figure 3.

Example. Finally, using $k = 2$, $u = 12$, and $\{u_1, u_2, u_3, u_4\}$ equal to $\{2, 3, 4, 6\}$, the techniques of our proof of Theorem 13 show that for p a prime, $p \equiv 1262 \pmod{4095}$, the graph $G_p^{(2)}$ always has a 12-cycle but never has cycles of lengths 2, 3, 4, or 6. The smallest p in this equivalence class is 21737. (This is the smallest prime that arises from the technique of Theorem 13, but it is not the smallest prime p such that $G_p^{(2)}$ has a cycle of length 12 but none of lengths 2, 3, 4, or 6; experimentation shows that the first such prime would be 53, not 21737. We will explain this further in a moment.)

One problem with the above examples (all of which arise from the techniques of Theorem 13) is that while they guarantee an infinite list of primes that satisfy the given requirements, it is not necessarily a complete list. For example, suppose we want to find all primes p such that for $G_p^{(2)}$ we have cycles of length 12, but no cycles of lengths 2, 3, 4, or 6. By our first example, we know any prime of the form $p \equiv 1262 \pmod{4095}$ will certainly work (and the first prime in this list is 21737). But as mentioned above, $p = 53$ works just fine as well. Let us see if

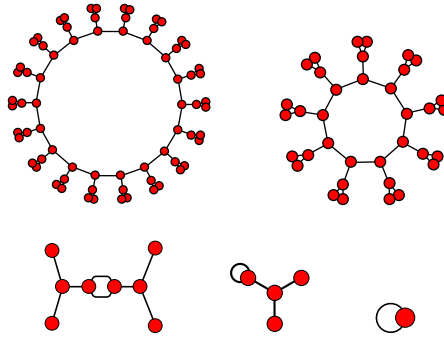


Figure 3. The digraph $G_{877}^{(2)}$ has eight components each of the forms shown in the top row, and just one component each of the forms shown in the bottom row. In particular, it has a 9-cycle but no 3-cycle.

we can demonstrate how to find all such primes p such that the digraphs $G_p^{(2)}$ will have cycles of length 12 but not length 2, 3, 4, or 6.

In order to find such p 's, we need

$$\gcd(2^{12} - 1, p - 1) > 1, \tag{3}$$

$$\gcd(2^6 - 1, p - 1) = 1, \tag{4}$$

$$\gcd(2^4 - 1, p - 1) = 1, \tag{5}$$

$$\gcd(2^3 - 1, p - 1) = 1, \tag{6}$$

$$\gcd(2^2 - 1, p - 1) = 1, \tag{7}$$

$$\gcd(2^1 - 1, p - 1) = 1. \tag{8}$$

By Lemma 14, we know there exists a prime divisor q such that $q \mid 2^{12} - 1$ but $q \nmid 2^i - 1$, where $i \in \{2, 3, 4, 6\}$, and a brief calculation shows $q = 13$. Therefore, we have $13 \mid \gcd(2^{12} - 1, p - 1)$ and so it follows that $p - 1 = 13n$, or $p = 13n + 1$. In order for (4)–(7) to hold, we must make sure that n does not contain any proper divisor of $(2^i - 1)$, where $i \in \{2, 3, 4, 6\}$; that is, 3, 5, and 7 must not divide n . So, a complete list of primes p can be written as the set

$$\{p \text{ is prime} : p = 13n + 1 \text{ where } n \in \mathbb{N} \text{ and } 3, 5, 7 \nmid n\}.$$

The smallest p is indeed 53.

If we glance at (3)–(8), we might wonder if we can modify them to give us more liberty in deciding what cycles we want to have and not have in our $G_p^{(k)}$. Suppose we want to change the above example to have a digraph with cycles of lengths 12 and 2, but no other cycles of lengths 3, 4, or 6. By Theorem 4, we need to start with

$$\gcd(2^{12} - 1, p - 1) > \gcd(2^2 - 1, p - 1) > 1.$$

Since $2^2 - 1 \mid 2^4 - 1$ and $2^2 - 1 \mid 2^6 - 1$, we know that $\gcd(2^4 - 1, p - 1)$ and $\gcd(2^6 - 1, p - 1)$ will both be at least as large as $\gcd(2^2 - 1, p - 1)$, but to prevent $G_p^{(2)}$ from having cycles of length 4 or length 6, we need them to be no larger than $\gcd(2^2 - 1, p - 1)$. Finally, to avoid any 3-cycles, we would like $\gcd(2^3 - 1, p - 1) = 1$. We can satisfy all these requirements if we are able to establish the six equations

$$\gcd(2^{12} - 1, p - 1) = q_2 q_{12}, \quad (9)$$

$$\gcd(2^6 - 1, p - 1) = q_2, \quad (10)$$

$$\gcd(2^4 - 1, p - 1) = q_2, \quad (11)$$

$$\gcd(2^2 - 1, p - 1) = q_2, \quad (12)$$

$$\gcd(2^3 - 1, p - 1) = 1, \quad (13)$$

$$\gcd(2^1 - 1, p - 1) = 1, \quad (14)$$

where q_2 and q_{12} are both primes. (Note the similarity between these six equations and the ones given earlier in (3)–(8).)

Fortunately, this is indeed possible. Lemma 14 guarantees that we can find appropriate primes q_2 and q_{12} ; our choices here will be $q_2 = 3$ and $q_{12} = 13$. We also need to ensure that $p - 1$ does not contain any other primes that might also appear in $2^k - 1$ as k runs over the divisors of 12. This can be satisfied by restricting ourselves to the set

$$\{p \text{ is prime} : p = 39n + 1 \text{ where } n \in \mathbb{N} \text{ and } 3, 5, 7 \nmid n\}.$$

It turns out the smallest such p is 79.

Naturally, we seek to generalize this technique, and the following theorem gives the appropriate conditions in which this can be done.

Theorem 15. *Let $u \geq 4$ be any composite number, let $k \geq 2$, and let $u' \geq 2$ be a proper divisor of u . So long as we do not have either $k = 2$ and $u' = 6$, or $k = 2$ and $u = 6$ and $u' = 3$, then there exist infinitely many primes p such that $G_p^{(k)}$ has both a u -cycle and a u' -cycle but has no w -cycle, where w is any other nontrivial proper divisor of u .*

Remark. The two restrictions in the above theorem are thanks to Theorem 13, which tells us that every digraph $G_p^{(2)}$ which contains a 6-cycle will also contain either a 2-cycle or 3-cycle, and that if it contains a 6-cycle and 3-cycle then it must also have a 2-cycle.

Proof of Theorem 15. We begin by considering the case where k is even and different from 2. This avoids the two exceptions to Lemma 14, and so we know there exist two separate primes q and q' such that $q \mid k^u - 1$ but $q \nmid k^w - 1$ for all $w < u$, and $q' \mid k^{u'} - 1$ but $q' \nmid k^w - 1$ for all $w < u'$. Since k is even, the primes q and q' are

necessarily odd. We want to set up a system similar to the ones in (9)–(14); in this context, our system will be

$$\gcd(k^u - 1, p - 1) = qq', \tag{15}$$

$$\gcd(k^y - 1, p - 1) = q' \quad \text{if } y < u \text{ and } y \text{ divisible by } u', \tag{16}$$

$$\gcd(k^z - 1, p - 1) = 1 \quad \text{if } z < u \text{ and } z \text{ not divisible by } u'. \tag{17}$$

(Here, y and z run over the proper divisors of u .) These three conditions, along with Theorem 4, would guarantee the existence of a cycle of length u and one of length u' and would prohibit any cycles of length w for w any other nontrivial divisor of u . It remains to show there are infinitely many such primes p that satisfy (15)–(17). Fortunately, this is not too hard. Let Q be the product of all the primes other than q and q' that divide $k^u - 1$. Since neither q nor q' divide $k^1 - 1$ and since $k > 2$, there is at least one such prime, and since k is even, all such primes in Q are odd primes. If we now require

$$p - 1 \equiv qq' \pmod{(qq')^2}, \tag{18}$$

$$p - 1 \equiv 1 \pmod{Q}, \tag{19}$$

then we are guaranteed (15)–(17), as we now briefly demonstrate.

- To begin with, (18) tells us that qq' divides into $p - 1$, but no higher power of q or q' does so. Also, (19) tells us that no other prime ρ that divides into Q will also divide into $p - 1$. Hence, the gcd's in (15)–(17) must be either 1, q , q' , or qq' .
- To establish (15), we note that by definition, both q and q' divide into $k^u - 1$.
- For (16), we note that q' divides into $k^{u'} - 1$, which divides into $k^y - 1$ for y divisible by u' , and that q does not divide into any $k^y - 1$ for $y < u$.
- As for (17), note that $k^z - 1$ is not divisible by q for any $z < u$. If $k^z - 1$ was divisible by q' , then q' would divide the gcd of $k^z - 1$ and $k^{u'} - 1$. This gcd is $k^d - 1$ where $d = \gcd(z, u')$ and since z is not divisible by u' then we know $d < u'$, but this contradicts our definition of q' . Hence, $k^z - 1$ is not divisible by either q or q' and so we have established (17).

We can now apply the Chinese remainder theorem to write (18) and (19) as $p - 1 \equiv A \pmod{Q(qq')^2}$ for some integer A , which implies

$$p \equiv 1 + A \pmod{Q(qq')^2}$$

Are we now able to apply Dirichlet's theorem to claim that there are infinitely many primes that satisfy the above equivalence? Almost! We need only ensure that $1 + A$ is relatively prime to $Q(qq')^2$. Since (18) tells us that $A \equiv 0 \pmod{q}$, then $A + 1 \equiv 1 \pmod{q}$, and the same holds for q' . Hence, $A + 1$ is relatively prime to q and to q' . Now let ρ be one of the primes that divides Q . We know from (19) that $A \equiv 1 \pmod{\rho}$,

which means $A + 1 \equiv 2 \pmod{\rho}$, but of course ρ is an odd prime, so $A + 1$ is relatively prime to ρ . We conclude that $A + 1$ is relatively prime to $Q(qq')^2$, and so we can apply Dirichlet's theorem to complete the proof (for this case where k even and $k > 2$).

Next, we consider $k = 2$, $u = 6$, and $u' = 2$. This is a very specific case, and if we set $p \equiv 19 \pmod{63}$ to be prime, it is easy to verify that all four of the equations

$$\gcd(2^6 - 1, p - 1) = 9, \tag{20}$$

$$\gcd(2^2 - 1, p - 1) = 3, \tag{21}$$

$$\gcd(2^3 - 1, p - 1) = 1, \tag{22}$$

$$\gcd(2^1 - 1, p - 1) = 1. \tag{23}$$

are satisfied. Naturally, there are infinitely such primes p (the first one is $p = 19$) and Theorem 4 tells us that $G_p^{(2)}$ will have a 6-cycle and a 2-cycle but never a 3-cycle.

Next, consider $k = 2$ with neither u nor u' equal to 6. Since this avoids the exceptions to Lemma 14, as before we can find the two separate primes q and q' such that $q \mid k^u - 1$ but $q \nmid k^w - 1$ for all $w < u$, and $q' \mid k^{u'} - 1$ but $q' \nmid k^w - 1$ for all $w < u'$. We would like to define Q to be the product of all primes ρ different from q and q' that divide $2^u - 1$, but it is possible that no such primes ρ exist (consider, for example, $q = 73$ a factor of $2^9 - 1$, and $q' = 7$ a factor of $2^3 - 1$: there are no other prime factors of $2^9 - 1$). If this is the case, simply set $Q = 1$ and proceed as before.

Next, consider when $k > 2$ is odd and we do not have $u' = 2$ and $k = 2^s - 1$ with $s \geq 2$. Lemma 14 gives us the primes q and q' as before, and since q and q' do not divide $k^1 - 1$ (by definition), both q and q' are odd primes. However, in our earlier work, (15)–(17) depended on some of the equations $\gcd(k^z - 1, p - 1)$ being equal to 1, but now that $k^z - 1$ is even, this is no longer possible. Instead, we will ask that $p \equiv 3 \pmod{4}$ (which will mean that $p - 1$ is divisible by 2 and not 4), and we seek to establish the system

$$\gcd(k^u - 1, p - 1) = 2qq', \tag{24}$$

$$\gcd(k^y - 1, p - 1) = 2q' \quad \text{if } y < u \text{ and } y \text{ divisible by } u', \tag{25}$$

$$\gcd(k^z - 1, p - 1) = 2 \quad \text{if } z < u \text{ and } z \text{ not divisible by } u'. \tag{26}$$

By Theorem 4 this will be sufficient to create our desired digraph $G_p^{(k)}$. But can we find primes p that satisfy (24), (25), and (26)? Of course! Let Q be the product of all the odd primes other than q and q' that divide $k^u - 1$, with the understanding that if no such primes exist then $Q = 1$. If we now require

$$p - 1 \equiv qq' \pmod{(qq')^2}, \tag{27}$$

$$p - 1 \equiv 1 \pmod{Q}, \tag{28}$$

$$p - 1 \equiv 2 \pmod{4}, \tag{29}$$

then we are guaranteed (24)–(26), as we now briefly demonstrate:

- As seen earlier, (27) tells us that qq' divides into $p - 1$, but no higher power of q or q' does so. Also, (28) tells us that no other prime ρ that divides into Q will also divide into $p - 1$. And, (29) guarantees that $2 \mid (p - 1)$ but 4 does not. These observations, along with $k - 1$ being even, tell us that the gcd's in (24)–(26) must be either 2, $2q$, $2q'$, or $2qq'$.
- To establish (24), we note that both $p - 1$ and $k^u - 1$ are divisible by q and q' .
- For (25), we note that q' divides into $k^{u'} - 1$, which divides into $k^y - 1$ for y divisible by u' , and that q does not divide into any $k^y - 1$ for $y < u$. This is identical to our proof for (16).
- Likewise, (26) is proved the same way as (17).

As before, we can now use the Chinese remainder theorem to write $p = 1 + A \bmod 4Q(qq')^2$ for some appropriate A , and it is easy to show that $1 + A$ and $4Q(qq')^2$ are relatively prime, thus allowing us to finish the proof by using Dirichlet's theorem.

The very last case to consider is when $k = 2^s - 1$ for $s \geq 2$, and $u' = 2$. The issue here is that $k - 1$ and $k^{u'} - 1$ will have exactly the same prime divisors (just to different powers) so we cannot find an appropriate prime q' as we did earlier, where q' was supposed to divide $k^{u'} - 1$ but not $k - 1$. Instead, we have to proceed as follows. First, choose a prime q such that $q \mid k^u - 1$ but $q \nmid k^w - 1$ for all $w < u$. Note that q is necessarily odd. We now seek to establish

$$\gcd(k^u - 1, p - 1) = 4q, \tag{30}$$

$$\gcd(k^y - 1, p - 1) = 4 \quad \text{if } y < u \text{ and } y \text{ divisible by } 2, \tag{31}$$

$$\gcd(k^z - 1, p - 1) = 2 \quad \text{if } z < u \text{ and } z \text{ not divisible by } 2. \tag{32}$$

To do this, we let Q be the (possibly empty) product of all the odd primes other than q that divide into $k^u - 1$, and we require

$$p - 1 \equiv q \pmod{q^2}, \tag{33}$$

$$p - 1 \equiv 1 \pmod{Q}, \tag{34}$$

$$p - 1 \equiv 4 \pmod{8}. \tag{35}$$

Once more, we can easily show that (33)–(35) imply (30)–(32):

- Equations (33)–(35) imply that $p - 1$ is divisible by q but not q^2 , by 4 but not 8, and by no other prime factor ρ of $k^u - 1$. Keeping in mind that k is odd, we see that the gcd's in (31) and (32) must be either 2 or 4, and in (30) we must have either $2q$ or $4q$.
- To establish that (30) is equal to $4q$ and not $2q$, we note that $k^u - 1$ is divisible by $k^2 - 1$, which (since $k = 2^s - 1$) is divisible by 4.

- For (31), we note again that $k^u - 1$ is divisible by 4.
- Finally, for z odd, $k^z - 1$ factors as $(k - 1)(k^{z-1} + k^{z-2} + \dots + 1)$. The first expression is $k - 1 = 2^s - 2$, which is divisible by 2 but not 4. The second expression is the sum of an odd number of odd terms, and hence odd. Thus, (32) is indeed equal to 2 and not 4.

As before, we summarize (33)–(35) as a single expression $p = 1 + A \pmod{8Qq^2}$ for some appropriate A , and it is now fairly routine to finish the proof by using Dirichlet's theorem. \square

Acknowledgment

The authors are grateful to the anonymous referees, who suggested many improvements and corrections that greatly improved this paper. In particular, the proof of Theorem 15 would not have been possible without their help.

References

- [Bang 1886] A. S. Bang, “Taltheoretiske undersøgelser”, *Tidsskrift f. Math.* **4**:5 (1886), 70–80, 130–137.
- [Gallian 2010] J. A. Gallian, *Contemporary abstract algebra*, 7th ed., Brooks/Cole, Belmont, CA, 2010.
- [Lucheta, Miller and Reiter 1996] C. Lucheta, E. Miller, and C. Reiter, “Digraphs from powers modulo p ”, *Fibonacci Quart.* **34**:3 (1996), 226–239. MR Zbl
- [Niven, Zuckerman and Montgomery 1991] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An introduction to the theory of numbers*, 5th ed., Wiley, New York, 1991. MR Zbl
- [Roitman 1997] M. Roitman, “On Zsigmondy primes”, *Proc. Amer. Math. Soc.* **125**:7 (1997), 1913–1919. MR Zbl
- [Somer and Křížek 2004] L. Somer and M. Křížek, “On a connection of number theory with graph theory”, *Czechoslovak Math. J.* **54(129)**:2 (2004), 465–485. MR Zbl
- [Somer and Křížek 2009] L. Somer and M. Křížek, “On symmetric digraphs of the congruence $x^k \equiv y \pmod{n}$ ”, *Discrete Math.* **309**:8 (2009), 1999–2009. MR Zbl
- [Wilson 1998] B. Wilson, “Power digraphs modulo n ”, *Fibonacci Quart.* **36**:3 (1998), 229–239. MR Zbl
- [Zsigmondy 1892] K. Zsigmondy, “Zur Theorie der Potenzreste”, *Monatsh. Math. Phys.* **3**:1 (1892), 265–284. MR Zbl

Received: 2014-01-21

Revised: 2017-06-08

Accepted: 2017-06-21

dresdeng@wlu.edu

*Department of Mathematics, Washington and Lee University,
Lexington, VA, United States*

wenda-tu@uiowa.edu

*Department of Statistics and Actuarial Science,
University of Iowa, Iowa City, IA, United States*

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

MANAGING EDITOR

Kenneth S. Berenhaut Wake Forest University, USA

BOARD OF EDITORS

Colin Adams	Williams College, USA	Suzanne Lenhart	University of Tennessee, USA
John V. Baxley	Wake Forest University, NC, USA	Chi-Kwong Li	College of William and Mary, USA
Arthur T. Benjamin	Harvey Mudd College, USA	Robert B. Lund	Clemson University, USA
Martin Bohner	Missouri U of Science and Technology, USA	Gaven J. Martin	Massey University, New Zealand
Nigel Boston	University of Wisconsin, USA	Mary Meyer	Colorado State University, USA
Amarjit S. Budhiraja	U of North Carolina, Chapel Hill, USA	Emil Minchev	Ruse, Bulgaria
Pietro Cerone	La Trobe University, Australia	Frank Morgan	Williams College, USA
Scott Chapman	Sam Houston State University, USA	Mohammad Sal Moslehian	Ferdowsi University of Mashhad, Iran
Joshua N. Cooper	University of South Carolina, USA	Zuhair Nashed	University of Central Florida, USA
Jem N. Corcoran	University of Colorado, USA	Ken Ono	Emory University, USA
Toka Diagana	Howard University, USA	Timothy E. O'Brien	Loyola University Chicago, USA
Michael Dorff	Brigham Young University, USA	Joseph O'Rourke	Smith College, USA
Sever S. Dragomir	Victoria University, Australia	Yuval Peres	Microsoft Research, USA
Behrouz Emamizadeh	The Petroleum Institute, UAE	Y.-F. S. Pétermann	Université de Genève, Switzerland
Joel Foisy	SUNY Potsdam, USA	Robert J. Plemmons	Wake Forest University, USA
Errin W. Fulp	Wake Forest University, USA	Carl B. Pomerance	Dartmouth College, USA
Joseph Gallian	University of Minnesota Duluth, USA	Vadim Ponomarenko	San Diego State University, USA
Stephan R. Garcia	Pomona College, USA	Bjorn Poonen	UC Berkeley, USA
Anant Godbole	East Tennessee State University, USA	James Propp	U Mass Lowell, USA
Ron Gould	Emory University, USA	József H. Przytycki	George Washington University, USA
Andrew Granville	Université Montréal, Canada	Richard Rebarber	University of Nebraska, USA
Jerold Griggs	University of South Carolina, USA	Robert W. Robinson	University of Georgia, USA
Sat Gupta	U of North Carolina, Greensboro, USA	Filip Saidak	U of North Carolina, Greensboro, USA
Jim Haglund	University of Pennsylvania, USA	James A. Sellers	Penn State University, USA
Johnny Henderson	Baylor University, USA	Andrew J. Sterge	Honorary Editor
Jim Hoste	Pitzer College, USA	Ann Trenk	Wellesley College, USA
Natalia Hritonenko	Prairie View A&M University, USA	Ravi Vakil	Stanford University, USA
Glenn H. Hurlbert	Arizona State University, USA	Antonia Vecchio	Consiglio Nazionale delle Ricerche, Italy
Charles R. Johnson	College of William and Mary, USA	Ram U. Verma	University of Toledo, USA
K. B. Kulasekera	Clemson University, USA	John C. Wierman	Johns Hopkins University, USA
Gerry Ladas	University of Rhode Island, USA	Michael E. Zieve	University of Michigan, USA

PRODUCTION

Silvio Levy, Scientific Editor


Cover: Alex Scorpan

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2018 is US \$190/year for the electronic version, and \$250/year (+\$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2018 Mathematical Sciences Publishers

involve

2018 vol. 11 no. 2

Finding cycles in the k -th power digraphs over the integers modulo a prime GREG DRESDEN AND WENDA TU	181
Enumerating spherical n -links MADELEINE BURKHART AND JOEL FOISY	195
Double bubbles in hyperbolic surfaces WYATT BOYER, BRYAN BROWN, ALYSSA LOVING AND SARAH TAMMEN	207
What is odd about binary Parseval frames? ZACHERY J. BAKER, BERNHARD G. BODMANN, MICAH G. BULLOCK, SAMANTHA N. BRANUM AND JACOB E. MCLANEY	219
Numbers and the heights of their happiness MAY MEI AND ANDREW READ-MCFARLAND	235
The truncated and supplemented Pascal matrix and applications MICHAEL HUA, STEVEN B. DAMELIN, JEFFREY SUN AND MINGCHAO YU	243
Hexatonic systems and dual groups in mathematical music theory CAMERON BERRY AND THOMAS M. FIORE	253
On computable classes of equidistant sets: finite focal sets CSABA VINCZE, ADRIENN VARGA, MÁRK OLÁH, LÁSZLÓ FÓRIÁN AND SÁNDOR LŐRINC	271
Zero divisor graphs of commutative graded rings KATHERINE COOPER AND BRIAN JOHNSON	283
The behavior of a population interaction-diffusion equation in its subcritical regime MITCHELL G. DAVIS, DAVID J. WOLLKIND, RICHARD A. CANGELOSI AND BONNI J. KEALY-DICHONE	297
Forbidden subgraphs of coloring graphs FRANCISCO ALVARADO, ASHLEY BUTTS, LAUREN FARQUHAR AND HEATHER M. RUSSELL	311
Computing indicators of Radford algebras HAO HU, XINYI HU, LINHONG WANG AND XINGTING WANG	325
Unlinking numbers of links with crossing number 10 LAVINIA BULAI	335
On a connection between local rings and their associated graded algebras JUSTIN HOFFMEIER AND JIYOON LEE	355



1944-4176(2018)11:2;1-7