1-2014

A Frobenius Question Related to Actions on Curves in Characteristic P

Darren B. Glass
Gettysburg College

Glass, Darren B. "A Frobenius Question Related to Actions on Curves in Characteristic P." Glasgow Mathematical Journal 56.1 (2014): 143-148.

A Frobenius Question Related to Actions on Curves in Characteristic P

Abstract
We consider which integers g can occur as the genus and of a curve defined over a field of characteristic p which admits an automorphism of degree pq, where p and q are distinct primes. This investigation leads us to consider a certain family of three-dimensional Frobenius problems and prove explicit formulas giving their solution in many cases.

Keywords
number theory, curves

Disciplines
Mathematics | Number Theory

Glasgow Math. J. **56** (2014) 143–148. © Glasgow Mathematical Journal Trust 2013.
doi:10.1017/S0017089513000128.

A FROBENIUS QUESTION RELATED TO ACTIONS ON CURVES IN CHARACTERISTIC *P*

DARREN B. GLASS

Department of Mathematics, Gettysburg College, Gettysburg, PA 17325, USA
e-mail: dglass@gettysburg.edu

(Received 26 June 2012; accepted 22 January 2013; first published online 13 August 2013)

Abstract. We consider which integers g can occur as the genus and of a curve defined over a field of characteristic p which admits an automorphism of degree pq, where p and q are distinct primes. This investigation leads us to consider a certain family of three-dimensional Frobenius problems and prove explicit formulas giving their solution in many cases.

2010 *Mathematics Subject Classification.* 11D07, 14G17, 11G20.

1. Introduction. A recent paper by O'Sullivan and Weaver [**5**] considers the largest genus in which no surface admits an automorphism of order n in the case $n = pq$, where p and q are distinct primes. In [**4**], the author begins considering the characteristic p analogue of this question by looking at curves that admit a $\mathbb{Z}/p\mathbb{Z}$-action and determining which genera g can occur for such curves as well as which p-ranks σ occur for a given genus.

In this paper we continue this investigation by considering curves defined over fields of characteristic p that admit a $\mathbb{Z}/pq\mathbb{Z}$-action, where q is a prime distinct from p. We note that these results generalize the results of [**3**], in which the author considers hyperelliptic curves admitting a $\mathbb{Z}/2m\mathbb{Z}$-action in characteristic 2 for all odd m and proves (among other things) the following result.

THEOREM 1.1. *For any odd integer m, there exist hyperelliptic curves of genus g defined over an algebraically closed field of characteristic* 2 *with automorphism group $\mathbb{Z}/2m\mathbb{Z}$ if and only if the least residue of g mod m is in the set $\left\{0, \frac{m-1}{2}, m-1\right\}$.*

In Section 2 of this paper we consider curves that admit a $\mathbb{Z}/pq\mathbb{Z}$-action in characteristic p, where q is a prime number distinct from p. The main approach in our investigation will be to assume that X admits a $\mathbb{Z}/pq\mathbb{Z}$-action with quotient Y, and consider the cover $X \to Y$ along with the $\mathbb{Z}/p\mathbb{Z}$ subcover, which we denote by C. We then use the Riemann–Hurwitz formula to compare the genera of X and Y. In particular, we show that if a curve of genus g admits such an action then $g + pq - 1 \in \langle pq, p\frac{q-1}{2}, \frac{p-1}{2}\rangle$. The bulk of Section 2 is dedicated to examining the converse question and giving sufficiency conditions on g. One example of such a result is the following.

COROLLARY 1.2. *If $g > \frac{p^2q-2pq+q}{2}$ and $g \equiv 1$ mod q then there exist curves of genus g which admit $\mathbb{Z}/pq\mathbb{Z}$-actions.*

In Section 3 we examine the Diophantine question asking what is the largest integer that cannot be expressed as a non-negative linear combination of $pq, p\frac{q-1}{2}$ and $\frac{p-1}{2}$. While our motivation for studying this question comes from the questions raised in Section 2, we believe that this problem is of independent interest. This is a special case of the Frobenius Problem, which in general asks for a description of sets $\langle a_1, \dots a_k\rangle$ of integers that can be expressed as the linear combination $a_1x_1 + \cdots a_kx_k$ for non-negative integer choices of x_i. In the case of $k = 2$, the answer is well known due to Sylvester **[6]**, and his result is standard in any undergraduate number theory text.

THEOREM 1.3. *Let a and b be fixed co-prime integers. Then any integer $d > ab - a - b$ can be expressed as a linear combination $d = ax + by$, where $x, y \in \mathbb{Z}_{\geq 0}$. Moreover, $ab - a - b \notin \langle a, b\rangle$ and exactly half of the integers between 1 and $ab - a - b + 1$ are in $\langle a, b\rangle$.*

However, the question becomes more difficult in the case where $k \geq 3$. In particular, while it is known that $\mathbb{Z}_{\geq 0} - \langle a_1, \dots a_k\rangle$ is a finite set, finding the largest number in this set is NP-hard for generic choices of a_i if $k \geq 3$ **[2]**. However, there are special cases of a_i for which a formula for the answer is known. This note hopes to add another case to the literature.

The author would like to thank Rachel Pries for her valuable suggestions.

2. Genera for $\mathbb{Z}/pq\mathbb{Z}$-actions. The main results in **[5]** consider Riemann surfaces admitting a $\mathbb{Z}/pq\mathbb{Z}$-action for odd prime numbers p and q. In particular, the authors show that there exists a curve of genus g admitting such an action if and only if $g - pq + 1 \in \langle pq, p'q, pq', \frac{pq-1}{2}\rangle$, where $p' = \frac{p-1}{2}$ and $q' = \frac{q-1}{2}$. They then go on to consider the four-dimensional Frobenius Problem related to the largest non-genus for such an action. Their proof carries over to positive characteristic fields as long as the characteristic of the base field is distinct from p and q. In this section we consider how their results change in the situation where our base field has characteristic p. We begin by proving a necessary condition on the genus of such a curve.

THEOREM 2.1. *Let X be a curve of genus g_X defined over an algebraically closed field of odd characteristic p admitting a $\mathbb{Z}/pq\mathbb{Z}$-action. Then $g_X + pq - 1 \in \langle pq, pq', p'\rangle$.*

Proof. Let C be the quotient of X by the $\mathbb{Z}/p\mathbb{Z}$ subgroup, and let Y be the quotient by the full $\mathbb{Z}/pq\mathbb{Z}$. Let us assume that there are b points which are fully ramified in the cover $X \to Y$. In particular, because both of these covers are Galois, we can assume that the cover $C \to Y$ is ramified at $b + c$ points and the cover $X \to C$ is ramified at $aq + b$ points. Applying the Riemann–Hurwitz formula to these covers we calculate that

$$\begin{aligned} g_X &= pg_C - (p-1) + p'R \\ &= p(qg_Y + (b+c)q' - (q-1)) - (p-1) + p'R \\ &= pqg_Y + pq'(b+c) + p'R - (pq-1), \end{aligned}$$

where R is the degree of the ramification divisor for the wild cover $X \to C$. The statement of the theorem follows. □

We note that the calculations in this proof will work in an identical manner if $p = 2$; however, in this case $p' = \frac{1}{2}$ making the results trivial if R is even and nonsensical if R is odd.

The natural question to ask is whether we get all linear combinations of pq, pq' and p' in the above construction. However, there is a non-trivial relationship between g_Y, b and R which makes the set of all possible genera somewhat smaller than the full set $\langle pq, pq', p'\rangle - (pq - 1)$. As an illustration of this, we note that if $b + c = 0$ then the cover $C \to Y$ is unramified and therefore $g_Y > 0$. Moreover, this would imply that $b = 0$, which in turn implies that R must be a multiple of q, eliminating a number of the genera in the set. We are, however, able to prove that curves admit $\mathbb{Z}/pq\mathbb{Z}$-actions under certain additional hypotheses.

THEOREM 2.2. *Assume that $p > 3$ and let $n \in \langle pq, p'q, pq'\rangle$ and $g = n + 5p'q + 1$. Then there exist curves of genus g which admit $\mathbb{Z}/pq\mathbb{Z}$-actions in characteristic p.*

Proof. Let Y be a hyperelliptic curve of genus at least one and let $C \to Y$ be a $\mathbb{Z}/q\mathbb{Z}$-cover ramified at c points. For any $y \in Y$ that is not a ramification point, there is a function on C which has poles of order two at q points lying above y; similarly, for any k that is not a multiple of p there will exist a function with exactly q poles each of order $2k$, leading to a ramification divisor of degree $(2k + 1)q$. One can similarly construct a function with q poles of order 2 and q poles of order $2k$ for any k such that $k \not\equiv 0 \pmod{p}$, giving a ramification divisor of degree $(2k + 4)q$. One is similarly able to construct functions with ramification degrees $(2k + 7)q$ and $(2k + 10)q$. Because $p > 3$, if $R = mq$, where $m > 4$, then R will take one of these forms and we can construct a cover ramified only at these points. We compute the genus of such a curve as follows:

$$\begin{aligned} g_X &= pqg_Y + pq'(b + c) + p'R - (pq - 1) \\ &= pqg_Y + pq'c + p'(mq) - pq + 1 \\ &= pq(g_Y - 1) + p'q(m - 5) + pq'c + 5p'q + 1. \end{aligned}$$

The theorem follows. □

Setting $c = 0$ and combining this result with Theorem 1.3 immediately yields the following result. In particular, we note that results in the next section will show that the bound of this sufficiency condition given is of the same order as those of the necessary conditions given in Theorem 2.1.

COROLLARY 2.3. *If $g > \frac{(p-1)(p+2)q}{2}$ and $g \equiv 1 \bmod q$, then there exist curves of genus g which admit $\mathbb{Z}/pq\mathbb{Z}$-actions.*

In order to get a different kind of sufficiency condition, we note that if $b \geq 1$ then this means that one or more of the ramification points of the cover $X \to C$ is a ramified point in the cover $C \to Y$ as well, allowing R to take on values that are not themselves multiples of q. In particular, for any such point on C, one can construct a function that has a pole of order $2q$ at this point by letting Y to be a hyperelliptic curve and lifting a function on Y with ramification type (2) to C. This in turn allows us to construct functions on C that have b poles and a ramification divisor whose degree is $R = 2lq + b$ for any $b \geq 1$ and $l \geq b$ with the only restriction that if $b = 1$ then l cannot be a multiple of p.

Following the example of the previous theorem, this allows us to construct curves X with $\mathbb{Z}/pq\mathbb{Z}$-actions with genus as follows:

$$\begin{aligned} g_X &= pqg_Y + pq'(b+c) + p'R - (pq-1) \\ &= pqg_Y + pq'b + pq'c + p'(2lq+b) - (pq-1) \\ &= pqg_Y + pq'c + 2p'q(l-b) + (pq' + 2p'q + p')b - pq + 1 \\ &= pqg_y + pq'c + (p-1)q(l-b) + \left(\frac{3pq-2q-1}{2}\right)b - pq + 1 \\ &= pqg_y + pq'c + (p-1)q(l-b) + \left(\frac{3pq-2q-1}{2}\right)(b-1) + \frac{pq-2q+1}{2}. \end{aligned}$$

We are able to make such a construction as long as we are not in the situation where $b = 1$ and $c = g_y = 0$. In particular, we have the following result.

THEOREM 2.4. *Let* $n \in \langle pq, pq', 2p'q, \frac{3pq-2q-1}{2}\rangle$ *and let* $g = n + \frac{pq-2q+1}{2} + \gamma$, *where* $\gamma \in \{pq, pq', \frac{3pq-2q-1}{2}\}$. *Then there exist curves of genus* g *which admit* $\mathbb{Z}/pq\mathbb{Z}$*-actions in characteristic* p.

Theorems 2.2 and 2.4 give several sets of conditions sufficient to construct curves admitting $\mathbb{Z}/pq\mathbb{Z}$-actions in characteristic p. We note that while the sets are not disjoint, each contains numbers that are not in the other. Moreover, there are genera that are not covered by either of these sufficiency conditions but are potential genera according to Theorem 2.1.

3. A certain Frobenius number. Let p and q be odd numbers and let $p' = \frac{p-1}{2}$ and $q' = \frac{q-1}{2}$. We are interested in computing the Frobenius number $Frob(pq, pq', p')$, which is the largest integer not contained in $\langle pq, p\frac{q-1}{2}, \frac{p-1}{2}\rangle$ and which we denote by $F(p, q)$. While there are algorithms to compute three-dimensional Frobenius numbers in general, this problem has some nice properties that we can exploit to get simple polynomial formulas in certain cases.

LEMMA 3.1. $F(p, 3) = \frac{p^2-4p+1}{2}$

Proof. The proof of this lemma is immediate from the fact that

$$F(p, 3) = Frob(3p, p, p') = Frob(p, p') = pp' - p - p'$$

□

THEOREM 3.2. *Set* $d = \frac{(q-1)(q-3)}{2}$ *and* $D = \frac{d^2-4d}{2} = \frac{(q+1)(q-1)(q-3)(q-5)}{8}$. *Then for all* $p \geq 2d$ *we have that* $F(p, q) = F(p + d, 3) - D$.

Proof. It follows from Lemma 3.1 that

$$\begin{aligned} F(p+d, 3) - D &= \frac{(p+d)^2 - 4(p+d) + 1}{2} - D \\ &= \frac{p^2 + (2d-4)p + (d^2 - 4d + 1)}{2} - \frac{d^2 - 4d}{2} \\ &= \frac{(p + 2d - 4)p + 1}{2}. \end{aligned}$$

We wish to show that $\frac{(p+2d-4)p+1}{2}$ cannot be written as a non-negative linear combination of pq, pq' and p'. We note that if it were then it would also be expressible as a non-negative linear combination $ap + bp'$, with the additional restriction that a was a non-negative linear combination of q and q'. Now assume that $\frac{(p+2d-4)p+1}{2} = ap + bp'$ so that $(p + 2d - 4)p + 1 = (2a + b)p - b$. In particular, this means that there must exist some k so that $2a + b - k = p + 2d - 4$ and $kp - b = 1$. Because a, b, d, p are all non-negative integers, it follows that k must be as well. One can solve this system of equations to see that $a = \frac{p+2d-3+k(1-p)}{2}$.

If $k = 1$, then one can solve to see that $a = d - 1$. However, $d - 1 = qq' - q - q'$, which by the classical solution to the two-dimensional Frobenius problem cannot be expressed as a non-negative linear combination of q and q', giving us a contradiction. On the other hand, if $k \geq 2$ then $a \leq \frac{2d-1-p}{2}$, which is impossible if $p \geq 2d$.

This shows that $\frac{p^2+(2d-4)p+1}{2}$ cannot be expressed as a non-negative linear combination of pq, pq', p'. Now assume that $x > \frac{p^2+(2d-4)p+1}{2}$. Then $x - dp > \frac{p^2-4p+1}{2} = pp' - p - p'$. In particular, $x - dp$ can be expressed as a non-negative linear combination of p and p'. But this implies that x can also be expressed as a non-negative linear combination $ap + bp'$, where $a > d$ and therefore a can be expressed as a non-negative linear combination of q and q'. This implies that x can be expressed as a non-negative linear combination of pq, pq', p' for all $x > \frac{p^2+(2d-4)p+1}{2}$, thereby proving that $F(p, q) = \frac{p^2+(2d-4)p+1}{2} = F(p + d, 3) - D$ as desired. □

The previous theorem can be used to give the following explicit formula for $F(p, q)$ for sufficiently large p.

COROLLARY 3.3. *If $p \geq (q - 1)(q - 3)$ then $F(p, q) = \frac{p^2-p+pq^2-4pq+1}{2}$.*

There are also reductions that one can make depending on the congruence class of q mod $p - 1$ regardless of the relative size of p and q.

LEMMA 3.4. *If $q \equiv 1 \ (mod\ p - 1)$ then $F(p, q) = \frac{p^2q-3pq-p+1}{2}$.*

Proof. Assume that $q = k(p - 1) + 1$. Then

$$\begin{aligned} F(p, q) &= Frob(kp(p - 1) + p, kpp', p') \\ &= Frob(kp(p - 1) + p, p'). \end{aligned}$$

Moreover, one can see that for any $d|p'$ we have $kp(p - 1) + p \equiv 1 \bmod d$ and therefore these numbers are relatively prime. This implies that $F(p, q)$ is equal to $kpp'(p - 1) + pp' - p' - kp(p - 1) - p$, which simplifies to the formula in the statement of the lemma. □

LEMMA 3.5. *If $q \equiv \frac{p-1}{2} \ (mod\ p - 1)$ then $F(p, q) = \frac{p^2q-3pq-p^2+p+2}{4}$.*

Proof. Assume that $q = k(p - 1) + p'$. Then

$$\begin{aligned} F(p, q) &= Frob\left((2k + 1)pp', \frac{(2k + 1)pp' - 2p}{4}, p'\right) \\ &= Frob\left(\frac{(2k + 1)pp' - 2p}{4}, p'\right) \\ &= \frac{p(p - 1)(p - 3)}{4}k + \frac{p^3 - 6p^2 + 5p + 4}{8}, \end{aligned}$$

which simplifies to the formula in the statement of the lemma. □

The previous two lemmata corresponded to the cases where $p'|q'$ and $p'|q$. This next lemma corresponds to the case where $q \equiv q' \bmod p'$.

LEMMA 3.6. *If* $q \equiv -1 \ (mod\ p-1)$ *then* $F(p,q) = \frac{4p^2-5p+2p^2q-6pq+2}{4}$.

Proof. Assume that $q = (p-1)k - 1$. Then we compute that $F(p,q) = Frob(p(p-1)k - p, pp'k - p, p')$. We note that both $p(p-1)k - p$ and $pp'k - p$ are congruent to $-1 \bmod p'$ and one can easily deduce that the smallest number congruent to $-a \bmod p'$ which is representable as a non-negative linear combination of these three numbers will be $a(pp'k - p)$. In particular, the last congruence class which is 'covered' will be $-a = 1$ and therefore the biggest number not representable is the Frobenius number $F(p,q) = \frac{p-3}{2}(pp'k - p) - p'$. This simplifies to the formula in the statement of the lemma. □

LEMMA 3.7. *If* $q \equiv 3 \ (mod\ p-1)$ *then* $F(p,q)$ *is given by the following formula:*

$$F(p,q) = \begin{cases} \frac{pp'q}{3} - p' - p & p \equiv 1 \bmod 6 \\ \frac{pp'q}{3} - p' - \frac{p}{2} - \frac{pq}{6} & p \equiv 3 \bmod 6 \\ \frac{pp'q}{3} - p' - \frac{pq}{3} & p \equiv 5 \bmod 6 \end{cases}.$$

The proof of this lemma relies on noting that if $pq \equiv 3 \bmod p-1$ and $pq' \equiv 1 \bmod p-1$ then when looking at linear combinations of pq and pq', the last congruence class mod p', which is 'covered', is $\frac{p-3}{2}$, which is first represented by $D = p\frac{q-3}{2}(\frac{p-3}{2} - \lfloor\frac{p-3}{6}\rfloor) + \frac{p(p-3)}{2}$. In particular, this means that $F(p,q) = D - p'$, which simplifies to the formula in the statement of the lemma. We note that this is a special case of the situation in [**1**], in which the author considers Frobenius numbers $Frob(x,y,z)$, where $x < y < z$ and $y \equiv 1 \bmod x$. Along the lines of the approach in that paper, one could, in principle, find an infinite set of polynomials $\{F_{a,b}(p,q)\}$ indexed by positive integers a, b in which $F(p,q) = F_{a,b}(p,q)$ as long as a is the least residue of $q \bmod p-1$ and b is the least residue of $p \bmod a$. However, as Byrne [**1**] points out, 'the details quickly become onerous', and other algorithms to solve these Frobenius numbers will in general be quite a bit faster.

REFERENCES

1. J. S. Byrnes, On a partition problem of Frobenius, *J. Comb. Theory Ser.* A **17** (1974), 162–166. MR 0347732 (50 #234).

2. F. Curtis, On formulas for the Frobenius number of a numerical semigroup, *Math. Scand.* **67**(2) (1990), 190–192. MR 1096454 (92e:11019).

3. D. Glass, The 2-ranks of hyperelliptic curves with extra automorphisms, *Int. J. Number Theory* **5**(5) (2009), 897–910. MR 2553515 (2010h:11100).

4. D. Glass, Non-genera of curves with automorphisms in characteristic p, in *Computational algebraic and analytic geometry*, Contemporary Mathematics, vol. 572 (Seppälä M. and Volcheck E., Editors) (American Mathematical Society, Providence RI, 2012), 89–95.

5. C. O'Sullivan and A. Weaver, A diophantine frobenius problem related to Riemann surfaces, *Glasg. Math. J.* **53**(3) (2011), 501–522. MR 2822795.

6. J. J. Sylvester, Question 7382, in *Mathematical questions from the educational times*, vol. 41 (1884).