Riemann-Hurwitz and Applications

Adam B Block

4 August, 2017

1 Introduction

The following is an important application of the theorem of Riemann and Roch. The Riemann-Hurwitz formula allows one to compare genera of nonsingular curves over algebraically closed fields and is used often in computations. We first set up some of the requisite commutative algebra and then prove the theorem. Following this, we present two applications of the formula, one to the abstract theory of fields and a surprising application to a version of Fermat's last theorem for polynomials. We fix the following notation in the sequel. All of our fields will be algebraically closed, we set $f : X \to Y$ as a finite separable morphism of two curves X, Y over k. All curves are nonsingular and projective. Note that the case $\operatorname{char} k > 0$ is included, but it is here that the separability condition must be checked carefully.

2 Some Commutative Algebra

2.1 Length of a Module

Much like we have a concept of dimension of a vector space, we wish to have a concept of 'dimension' of a more general R-module. We call this notion the length.

Definition 1. Let M a finite R-module. Then M has a Jordan-Hölder decomposition of well-defined length l. Let $l(M) = l$. In particular, l is the maximal n such that there exists a chain

$$0 = M_0 \subsetneq M_1 \subsetneq ... \subsetneq M_l = M$$

or, equivalently is the length of such an ascending chain where M_i/M_{i-1} is simple.

Remark 2. Note that if $R = k$ a field then M becomes a vector space and it is easy to check that $l(M) = \dim_k M$, thus making length a true generalization of dimension.

We use the following lemma to calculate length of modules over certain types of rings.

Lemma 3. *Let $(R, \mathfrak{m})$ be a valuation domain. Then let $M = R/\mathfrak{m}^e$ Then $l(M) = e$.*

Proof. Identify the ideals $\mathfrak{m}^i \subset R$ with their images in $R/\mathfrak{m}^e$. Then consider the ascending chain

$$0 = \mathfrak{m}^e/\mathfrak{m}^e \subsetneq \mathfrak{m}^{e-1}/\mathfrak{m}^e \subsetneq ... \subsetneq R/\mathfrak{m}^e = M$$

Letting $M_i = \mathfrak{m}^{e-i}/\mathfrak{m}^e$, we see that $M_i/M_{i-1} \cong \mathfrak{m}^{e-i}/\mathfrak{m}^{e-i+1}$ which is a one dimensional vector space over $R/\mathfrak{m}$, so M_i/M_{i-1} is simple. ∎

There is much more to be said about lengths of modules; the curious reader is referred to a good book on commutative algebra, with Matsumura's and Eisenbud's being especially recommended.

2.2 Invertible Modules and Divisors

Recall that localization at a multiplicatively closed subset is functorial and is exact, meaning that if $S \subset R$ is a multiplicatively closed subset and M, M', M'' are R modules, and

$$0 \longrightarrow M'' \longrightarrow M \longrightarrow M' \longrightarrow 0$$

is exact, then

$$0 \longrightarrow S^{-1}M'' \longrightarrow S^{-1}M \longrightarrow S^{-1}M' \longrightarrow 0$$

is also exact. Moreover, we have a canonical isomorphism for two R-modules M, N

$$S^{-1}(M \otimes N) \simeq (S^{-1}M) \otimes (S^{-1}N)$$

We now define

Definition 4. Let R be a Noetherian ring and M a finite R-module. Then the *support* of M, $\operatorname{Supp}(M)$ is the set of prime ideals $\mathfrak{p} \in \operatorname{Spec} R$ such that $M_\mathfrak{p} \neq 0$.

We make use of the following proposition.

Proposition 5. *Let R be a ring and M a finite R-module with $m \in M$. Let $\mathfrak{p} \subset R$ be a prime ideal and let $m_\mathfrak{p}$ denote the image of m in $M_\mathfrak{p}$. Then $m_\mathfrak{p} \neq 0$ if and only if $\operatorname{Ann}(m) \subset \mathfrak{p}$. Thus $m = 0$ if and only if $m_\mathfrak{p} = 0$ for all $\mathfrak{p} \in \operatorname{Spec} R$. More generally, $M_\mathfrak{p} \neq 0$ if and only if $\operatorname{Ann}(M) \subset \mathfrak{p}$ and so $M_\mathfrak{p} = 0$ for all $\mathfrak{p} \in \operatorname{Spec} R$ if and only if $M = 0$. Thus $\operatorname{Supp}(M) = V(\operatorname{Ann}(M))$ and in particular $\operatorname{Supp}(M)$ is closed in the Zariski topology.*

Proof. The first statement follows from the statement that if $a \in \operatorname{Ann}(m)$ then $m = \frac{a}{a}m = 0$ so if $a \notin \mathfrak{p}$ then $m_\mathfrak{p} = 0$. The converse is easy. We note that $m = 0$ if and only if $\operatorname{Ann}(m) = R$ which is true if and only if there is no prime $\mathfrak{p}$ such that $\operatorname{Ann}(m) \subset \mathfrak{p}$, proving the second statement. The corresponding statments on finite modules can be passed to the case of generators and the last statement is immediate. ■

Now it behooves us to introduce a concept that may seem unmotivated. For those that are interested in the reason we make use of this definition, I recommend the study of schemes.

Definition 6. Let M be an R-module. We say that M is locally free if for all $\mathfrak{p} \in \operatorname{Spec} R$, there exists an element $f \notin \mathfrak{p}$ such that for some $r \in \mathbb{N}$, $M_f \cong R_f^{\oplus r}$. If R is irreducible, then it is clear that r is constant and we say that M is *locally free of rank r*. If M is locally free of rank 1, we say that M is *invertible*.

Remark 7. The reasoning behind calling M invertible is that if we let $M^\vee = \operatorname{Hom}(M, R)$ then we get that $M \otimes M^\vee \cong R$. Because $R \otimes M \cong M$, we can form the *Picard Group*, $\operatorname{Pic} R$, as the set of isomorphism classes of invertible modules with group operation the tensor product. It is easy to check that this is an abelian group.

While the definition above may seem a little bit odd to one unfamiliar with algebraic geometry, it should be clear why the picard group is important after the following proposition.

Proposition 8. *Let X be a curve over k and let $\operatorname{Cl} X$ be the class group. Let M be an invertible $\mathcal{O}_X$ module. Every such module is given up to isomorphism by a set of pairs (f_i, g_i) such that $f_i \in \mathcal{O}_X$ such that the set of f_i generates the unit ideal, $g_i \in (\mathcal{O}_X)_{f_i}^\times$ and for each i, j, the element $g_i/g_j \in (\mathcal{O}_X)_{f_i f_j}^\times$. Then there is an isomorphism $\phi : \operatorname{Pic} \mathcal{O}_X \to \operatorname{Cl} X$ given by*

$$M \mapsto \sum_{\substack{P \in X \\ f_i \notin \mathfrak{p}}} v_P(g_i) \cdot P$$

where the sum is finite because $\mathcal{O}_X$ is Noetherian.

Proof. This is a pretty easy exercise. First check that the map is well-defined. After this, showing that it is an isomorphism is easy. ■

We conclude our discussion of algebra with the study of differentials.

2.3 Kähler Differentials

We begin with some commutative algebra, in particular, we define the *module of differentials*.

Definition 9. Let B be an A-algebra. Then we define an A-derivation as an A linear map $d : B \to M$ for some B-module M that satisfies

$$d(bb') = bdb' + b'db$$
$$d(a) = 0$$

We define the *Kähler differentials* to be the module of universal derivations, i.e., there is a derivation called the *exterior derivative* $d : B \to \Omega_{B/A}$ such that if $d' : B \to M$ is a derivation, then there exists a unique $\phi : \Omega_{B/A} \to M$ such that the following diagram commutes

$$\begin{tikzcd} B \arrow[r, "d"] \arrow[d, "d'"] & \Omega_{B/A} \arrow[dl, dashed, "\phi"] \\ M & \end{tikzcd}$$

We recall without proof the following proposition from commutative algebra:

Proposition 10. *Let $A \xrightarrow{f} B \xrightarrow{g} C$ be morphisms of rings. Then we have*

$$\Omega_{B/A} \otimes_B C \xrightarrow{\alpha} \Omega_{C/A} \xrightarrow{\beta} \Omega_{C/B} \longrightarrow 0$$

Where the map α is given by $\alpha(da \otimes b) = bd(g(a))$ and β is projection.

Proof. Find a good commutative algebra textbook. ■

Remark 11. As will soon become clear, in our case, we will essentially always be applying Proposition 10 in the case $A = k$ with B, C as k-algebras and the morphism $B \to C$ given by a morphism of varieties.

We will be making use of the following proposition:

Proposition 12. *Let K/k be a finite, separable extension. Then $\dim_K \Omega_{K/k} = \operatorname{tr.deg.} K/k$.*

Proof. Find a good commutative algebra textbook. ■

Remark 13. If K/k is not separable then we get a strict inequality $\dim_K \Omega_{K/k} > \operatorname{tr.deg.} K/k$.

Recall that we have an equivalence between finite type k-algebras and varieties over k that preserves dimension as transcendence degree. This leads us to the definition

Definition 14. Let X/k be a curve and let $B = \mathcal{O}_X$ be the coordinate ring of X. We let $\Omega_{X/k} = \Omega_{\mathcal{O}_X/k}$. For any point $P \in X$ defined by ideal $\mathfrak{p} \subset \mathcal{O}_X$, we define $\Omega_{X,P} = (\Omega_X)_{\mathfrak{p}}$. Given a morphism $f : X \to Y$ of curves over k, we let $\Omega_{X/Y} = \Omega_{\mathcal{O}_X/\mathcal{O}_Y}$ with $\Omega_{X/Y,P} = (\Omega_{X/Y})_{\mathfrak{p}}$ where the point $P \in X$ is given by the ideal $\mathfrak{p}$ and we let $f^*\Omega_Y = \Omega_Y \otimes_{\mathcal{O}_Y} \mathcal{O}_X$ be base extension, with localization analogous to the above.

For our purposes, the above definition will suffice, as we will be restricting our focus to curves. Before we move on, we consider the notion of det as a morphism of R-modules.

Definition 15. Let M be a locally free R-module of rank r. We define $\det M = \bigwedge^r M$. Thus $\det M$ is an invertible module.

Note that this definition of the determinant corresponds to our notion in that if M is a vector space and $\phi : M \to M$ is a morphism, then $\det \phi = \det(M)$ in the usual sense. We have that det behaves well with respect to exact sequences.

Proposition 16. *Let M, M', M'' be locally free R modules such that we have an exact sequence*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

Then $\det M \cong (\det M') \otimes (\det M'')$.

Proof. Because localization is exact, it suffices to check on free modules. Then the proof is trivial by choosing bases. ■

Letting $\omega_X = \det \Omega_X$, we note that $\omega_X \mapsto K_X$, the canonical class. In our case, we refer only to curves, and so $\Omega_X = \omega_X$, but this is not true in higher dimensions. We are now ready to proceed with the geometry.

3 Riemann-Hurwitz

We entirely restrict our attention to curves. In the sequel, let X, Y be nonsingular projective curves and let all morphisms be finite and separable (for those who do not know what these words mean, take *finite* to mean that general points have finite preimages and consider our work only over characteristic 0 to allow for us ignoring separable.) We begin with

Lemma 17. *Let $f : X \to Y$ be a morphism. Then we have a short exact sequence*

$$0 \longrightarrow f^*\Omega_Y \longrightarrow \Omega_X \longrightarrow \Omega_{X/Y} \longrightarrow 0$$

Proof. By Proposition 10, it suffices to prove injectivity of the first map. By Proposition 5, it suffices to demonstrate this injectivity after localizing at the minimal prime, namely $(0) \subset \mathcal{O}_X$. For convenience of notation, we drop the localization at 0 from our notation, but all modules should be taken to be over $K(X)$. We have $\Omega_Y = \Omega_{K(Y)/k}$ and $\Omega_X = \Omega_{K(X)/k}$ so by Proposition 12 and the fact that $\operatorname{tr.deg.} K(Y)/k = \operatorname{tr.deg.} K(X)/k = 1$, we get that $\dim_{K(X)} f^*\Omega_Y = \dim_{K(X)} \Omega_X = 1$ so it suffices to prove that the map $f^*\Omega_Y \to \Omega_X$ is nonzero. However, we have that $\Omega_{X/Y} = \Omega_{K(X)/K(Y)}$ is separable and finite so algebraic so by Proposition 12, $\dim \Omega_{X/Y} = 0$ so $\Omega_{X/Y} = 0$. By exactness in the second term given by Proposition 10, we have that $f^*\Omega_Y \to \Omega_X$ is surjective and so it is nonzero and we are done. ■

For the remainder of the section, we will find it convenient to fix notation. Let $f : X \to Y$ a morphism of curves such that $P \in X$, and $Q = f(P) \in Y$. Let t be a local parameter at Q and let u be a local parameter at P. Then we see immediately that $\Omega_{Y,Q}$ is generated over $\mathcal{O}_{Y,Q}$ by dt and $\Omega_{X,P}$ is generated over $\mathcal{O}_{X,P}$ by du. We thus get that there exists a unique $g \in \mathcal{O}_P$ such that $f^*dt = gdu$. We define $dt/du = g$. We now have the key proposition relating $\Omega_{X/Y}$ to ramification.

Proposition 18. *Let $f : X \to Y$ be a finite, separable morphism of curves. Let $\operatorname{char} k \nmid e_P$ for all $P \in X$. Then $\operatorname{Supp} \Omega_{X/Y} = \{\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_X | e_P > 1\}$ and $(\Omega_{X/Y})_P$ is principal with length $v_P(dt/du) = e_P - 1$.*

Proof. From Lemma 17, we have a short exact sequence

$$0 \longrightarrow f^*\Omega_Y \longrightarrow \Omega_X \longrightarrow \Omega_{X/Y} \longrightarrow 0$$

and localizing is exact, so we get

$$(\Omega_{X/Y})_P \cong (\Omega_X/f^*\Omega_{X/Y})_P \cong (\Omega_X)_P/(f^*\Omega_Y)_P$$

But we know that $(\Omega_X)_P = \mathcal{O}_P \cdot du$ and $(f^*\Omega_Y)_P = \mathcal{O}_P \cdot (\frac{dt}{du}du)$. Thus their quotient is just $\mathcal{O}_P/(\frac{dt}{du})$. Note that $\mathcal{O}_P/(\frac{dt}{du}) \neq 0$ if and only if $\frac{dt}{du}$ is not a unit if and only if $v_P(\frac{dt}{du}) > 0$. Thus $\Omega_{X/Y}$ has support precisely when $v_P(\frac{dt}{du}) > 0$. Thus it will suffice to show that $v_P(\frac{dt}{du}) = v_P(t) - 1 = e_p - 1$. Now suppose that f has ramification index e at P so $t = au^e$ for some $a \in \mathcal{O}_P^\times$. Then by the Leibniz rule,

$$dt = aeu^{e-1}du + ae^u da = u^{e-1}(aedu + auda)$$

But $a \in \mathcal{O}_P^\times$ so $v_P(a) = 0$. Thus we get that $v_P(\frac{dt}{du}) = e - 1$ as desired. Applying Lemma 3 yields the last statement. ■

Remark 19. When the condition $\operatorname{char} k \nmid e_P$ is satisfied, we say that the point P is *tamely ramified*; otherwise, we say that P is *wildly ramified*. We generally use the result for $k = \mathbb{C}$ so this is not such an important point for our purposes, but it should be noted that if P is wildly ramified then $v_P(dt/du) > e_P - 1$. To see this, note that in the calculation of dt, we get that $\operatorname{char} k | e$ so $e = 0 \in k$ and so the first term drops out, yielding $dt = au^e da$. But then we see that $l(\Omega_{X/Y})_P > e_P - 1$.

Corollary 20. *If $f : X \to Y$ is a finite separable morphism of curves, then there are finitely many ramified points.*

Proof. By Proposition 18 we have that $\operatorname{Supp} \Omega_{X/Y}$ is given exactly by the ramification points. But we know that $\operatorname{Supp} \Omega_{X/Y}$ is closed by Proposition 5 and closed sets in X that are not all of X are finite. But we know that $\Omega_{X/Y}$ is not supported everywhere because $(\Omega_{X/Y})_{(0)} = 0$ by the proof of Lemma 17. ■

By Corollary 20, we can take sums over ramification points and be assured that they are finite. Thus, we let

Definition 21. We define the *ramification divisor* to be

$$R = \sum_{P \in X} l((\Omega_{X/Y})_P) \cdot P$$

Remark 22. Note that the above definition is valid because if $P' \in X$ is unramified, then $l((\Omega_{X/Y})_{P'}) = 1 - 1 = 0$ and so this is just a sum over ramification points.

We now arrive at the first part of the main theorem.

Theorem 23 (Riemann-Hurwitz)**.** *Let $f : X \to Y$ be a finite separable morphism of curves. Let K_X, K_Y be the canonical divisors for X, Y respectively. Then*

$$K_X \sim f^* K_Y + R$$

Proof. From Lemma 17, we have an exact sequence,

$$0 \longrightarrow f^*\Omega_Y \longrightarrow \Omega_X \longrightarrow \Omega_{X/Y} \longrightarrow 0$$

From Proposition 16, we get $\det \Omega_X \cong \det f^*\Omega_Y \otimes \det \Omega_{X/Y}$. But formation of exterior powers commutes with base extension so we get $\omega_X \cong f^*\omega_Y \otimes \det(\Omega_{X/Y})$. Let D be the divisor associated to $\det(\Omega_{X/Y})$ under the mapping in Proposition 8. Then we get that $K_X \sim f^*K_Y + D$ and it suffices to show that $D = R$. To do this, it suffices to consider the result locally at any point $P \in X$. But $(\Omega_{X/Y})_P \cong \det(\Omega_{X/Y})_P$ and we have by Proposition 18 that $l(\Omega_{X/Y})_P = v_P(dt/du)$ so we are done. ■

Corollary 24 (Riemann-Hurwitz)**.** *Let $f : X \to Y$ be a finite separable morphism of curves with all ramification tame. Then*

$$2g_X - 2 = (\deg f)(2g_Y - 2) + \sum_{P \in X} e_P - 1$$

Proof. We know that $\deg K_X = 2g_X - 2$ and similarly for K_Y. We know that $\deg f^*K_Y = (\deg f) \deg K_Y$ and Proposition 18 gives us in the case of tame ramification $l((\Omega_{X/Y})_P) = e_p - 1$. Thus this follows trivially from Theorem 23 and the fact that degree is defined up to rational equivalence. ■

Remark 25. Note that in general Theorem 23 applies, although the proof may be slightly different. The separability condition becomes important in Corollary 24 where the equality turns into an inequality because of the discussion in Remark 19 and we instead get

$$2g_X - 2 > (\deg f)(2g_Y - 2) + \sum_{P \in X} e_P - 1$$

This last is the traditional degree formula of Riemann and Hurwitz. We now proceed to a few examples.

4 Applications

4.1 Lüroth's Theorem

Our first application of Riemann-Hurwitz is to a theorem from algebra called *Lüroth's Theorem.* Note that in general, the theorem holds for all fields, not just algebraically closed ones, but our proof only holds for the latter case because the work up to this point has had this assumption. We first need a few lemmata.

Lemma 26. *Let X be a curve such that $P, Q \in X$ are distinct points such that $P \sim Q$. Then $X \cong \mathbb{P}^1$.*

Proof. By definition of rational equivalence, $P \sim Q$ implies that there exists some $f \in K(X)$ such that $(f) = P - Q$. Then we have that $k(f) \hookrightarrow K(X)$ induces a map $\phi : X \to \mathbb{P}^1$. Letting $O = [0 : 0 : 1]$, note that $\phi^* O = P$ so $\deg \phi = 1$, which means that ϕ is birational. But nonsingular rational curves are isomorphic to $\mathbb{P}^1$ so we are done. ∎

Lemma 27. *Let X be a curve of genus 0. Then $X \cong \mathbb{P}^1$.*

Proof. If X is a curve of genus 0, let P, Q be distinct points and let $D = P - Q$. Then we note that $\deg D = 0$, and $\deg K = 2g - 2 = -2$ and so $l(K - D) = 0$. Applying Riemann-Roch, we see that $l(D) - 0 = 0 + 1 - 0 = 1$. Thus we have $D \sim 0$ meaning that $P \sim Q$. We are done by Theorem 26 ∎

Lastly, we need a result relating genera of two curves.

Lemma 28. *Let $f : X \to Y$ a finite morphism of curves. Then $g_X \geq g_Y$.*

Proof. If $g_Y = 0$ then this is clear because $g \geq 0$. Otherwise, $g_Y \geq 1$ and by Corollary 24, we have $2g_X - 2 = \deg f(2g_Y - 2) + \sum e_P - 1$. Solving for g_X, we have

$$g_X \geq g_Y + (\deg f - 1)(g_Y - 1) + \frac{\sum e_P - 1}{2}$$

But $\deg f \geq 1$ and $g_Y - 1 \geq 0$ so we are done. ∎

Remark 29. Note that the above proof gives the stronger statement that for f separable we achieve equality in genera if and only if $\deg f = 1$ and f is unramified.

We are now ready to proceed to the proof of Lüroth's theorem.

Theorem 30 (Lüroth)**.** *Let $k \subset L \subset k(t)$ be a tower of fields with $k = \overline{k}$. Then L is purely transcendental.*

Proof. We may assume that $k \neq L$ so $\operatorname{tr.deg.}_k L > 0$ by k being algebraically closed. But $\operatorname{tr.deg.} L \leq 1$ because $L \subset k(t)$ so $\operatorname{tr.deg.}_k L = 1$. But now we have that there exists a curve X/k such that $L = K(X)$. The morphism $L \hookrightarrow k(t)$ induces a morphism $\phi : \mathbb{P}^1 \to X$. By Lemma 28, we have $0 \leq g_X \leq 0 = g_{\mathbb{P}^1}$. By Lemma 27, $X \cong \mathbb{P}^1$. But then $L \cong k(t)$ so there exists some $u \in L$ such that $L = k(u)$ and we are done. ∎

4.2 Fermat's Last Theorem for Polynomials

As another application, we prove a version of Fermat's Last Theorem, but for polynomials. Consider the following.

Theorem 31. *Let k be an algebraically closed field and $f, g, h \in k[s, t]$ be nonconstant homogeneous polynomials such that $f^n + g^n = h^n$ with $\operatorname{char} k \nmid n$. Then $n \leq 2$.*

Proof. We first introduce the set $Y = V_+(x^n + y^n - z^n) \subset \mathbb{P}^2$, i.e., we have $Y = \{[s : t : z] : s^n + t^n = z^n\}$ and consider the morphism $\pi : Y \to \mathbb{P}^1$ projection onto the first two factors, i.e, $\pi([s : t : z]) = [s : t]$. We will use Corollary 24 to determing g_Y. Recall that

$$\sum_{P \mapsto Q} e_P = \deg \pi$$

and that for any point $[s : t : z] \in Y \cap U_2$, we have $[s : \zeta_n^i t : z] \in Y \cap U_2$ as well and so for $[s : t] \in \mathbb{P}^1$ such that $s^n + t^n \neq 0$, we have n distinct points $P_i' = [s : \zeta_n^i t : z] \in \pi^{-1}([s : t])$. Thus $\deg \pi = n$. We must now consider the branch locus. The branch locus is the set of all $Q_i \in \mathbb{P}^1$ such that $s^n + t^n = 0$. Clearly there are precisely n such points $Q_i = [1 : \zeta_n^i]$. Moreover, $\pi^{-1}(Q_i) = \{[1 : \zeta_n^i : 0]\} = \{P_i\}$. By Equation (4.2), we must have $e_{P_i} = n$. Thus there are n ramification points each of index n. By Corollary 24, we get

$$2g_Y - 2 = \deg \pi(2g_{\mathbb{P}^1} - 2) + \sum_{P \in X} e_P - 1$$

Plugging in our known values we get

$$2g_Y - 2 = n(-2) + n(n-1)$$

and solving for g_Y gives

$$g_Y = \frac{(n-1)(n-2)}{2}$$

Now suppose that f, g, h are nonconstant and satisfy Fermat's identity. Then we can define a finite map $\phi : \mathbb{P}^1 \to Y$ given by

$$\phi([s : t]) = [f(s,t) : g(s,t) : h(s,t)]$$

By Lemma 28, we know that $0 = g_{\mathbb{P}^1} \geq g_Y \geq 0$. Thus we have $0 = \frac{(n-1)(n-2)}{2}$ and we are done. ■

Remark 32. Note that if $\operatorname{char} k | n$ then we lose our separability hypothesis and the theorem fails. To see that it fails, let f, g, h be nonconstant polynomials such that $f + g = h$. Then we note that $f^{p^r} + g^{p^r} = h^{p^r}$ by Frobenius and p^r gets arbitrarily large.