respectively (where $u_{i_1,\dots,i_{N-1}}, v_{j_1,\dots,j_{N-1}} \in \overline{\mathbb{F}}_\ell[X_N]$ and neither $u_{R_1,\dots,R_{N-1}}$ nor $v_{T_1,\dots,T_{N-1}}$ is identically zero), we thus find that $u_{i_1,\dots,i_{N-1}}(\theta) = v_{j_1,\dots,j_{N-1}}(\theta) = 0$ for any $(i_1,\dots,i_{N-1}) \neq (0,\dots,0)$, $(j_1,\dots,j_{N-1}) \neq (0,\dots,0)$, and any $\theta$ as above. Thus, if the tuples $(R_1,\dots,R_{N-1})$ and $(T_1,\dots,T_{N-1})$ are both nonzero, then $\prod_{\substack{\theta\in\overline{\mathbb{F}}_\ell \\ F(\theta)=0}} (X_N-\theta)$ divides $u_{R_1,\dots,R_{N-1}}(X_N)$ and $v_{T_1,\dots,T_{N-1}}(X_N)$ in $\overline{\mathbb{F}}_\ell[X_N]$. But then, if $\alpha \in \mathbb{Z}$ is the leading coefficient of $F$, then comparing the monomials (in $X_1,\dots,X_{N-1}$) with maximal total degree in (10.1), we find that $\alpha^{N-1}F(X_N) = u_{R_1,\dots,R_{N-1}}(X_N)\, v_{T_1,\dots,T_{N-1}}(X_N) \equiv 0 \pmod{\prod_{\substack{\theta\in\overline{\mathbb{F}}_\ell \\ F(\theta)=0}} (X_N-\theta)^2}$, which is impossible by the observations in the first paragraph of the proof. This forces one of $(R_1,\dots,R_{N-1})$ or $(T_1,\dots,T_{N-1})$ to be $(0,\dots,0)$, say the latter. Then $V(X_1,\dots,X_N) = v_{0,\dots,0}(X_N)$ and since $N \geq 2$, plugging $X_1 := \theta$ for some root $\theta \in \overline{\mathbb{F}}_\ell$ of $F$ into (10.1) yields $-w = U(\theta, X_2,\dots,X_N)v_{0,\dots,0}(X_N)$, forcing $V$ to be identically constant.

*Proof of (b).* We claim that for all primes $\ell \gg_{F,G} 1$, if the rational function $F^aG^b$ is constant in the ring $\overline{\mathbb{F}}_\ell(T)$ for some integers $a, b$, then $a \equiv b \equiv 0 \pmod{\ell}$.[8] The argument for this is a simple variant of that given for the inequality "$\mathrm{ord}_\ell(\widetilde{F}) \leq \mathbb{1}_{\ell\leq C_1}C_1$" in the proof of Proposition 5.3(b), so we only sketch the outline. Since $\{F, G\} \subset \mathbb{Z}[T]$ are multiplicatively independent, the polynomials $\{F'G, FG'\} \subset \mathbb{Z}[T]$ are $\mathbb{Q}$-linearly independent, hence so are the columns of the matrix $M_1$ listing the coefficients of $F'G$ and $FG'$ in two columns. Hence we can find invertible matrices $P_1$ and $Q_1$ (where $Q_1$ is a $2\times 2$ matrix) such that $P_1M_1Q_1 = \mathrm{diag}(\beta_1,\beta_2)$ for some $\beta_1, \beta_2 \in \mathbb{Z}\setminus\{0\}$ satisfying $\beta_1 \mid \beta_2$. Let $\ell > |\beta_2|$ be any prime not dividing the leading coefficients of $F$, $G$, $F'G$ or $FG'$. If $F^aG^b$ is identically constant in $\mathbb{F}_\ell[T]$, then $aF'G+bFG' \equiv 0$ in $\mathbb{F}_\ell[T]$, so $M_1(a\ b)^\top \equiv 0 \pmod{\ell}$. Hereafter, familiar calculations yield $(a\ b)^\top \equiv 0 \pmod{\ell}$.

Collecting our observations, we have shown that there exists a constant $\kappa_1(F,G)$ such that for all primes $\ell > \kappa_1(F,G)$, the following three properties hold:

(i) $\ell > \kappa_0(F)$, so that $\prod_{\substack{\theta\in\overline{\mathbb{F}}_\ell \\ F(\theta)=0}} (T-\theta)^2 \nmid F(T)$ in $\overline{\mathbb{F}}_\ell[T]$;

(ii) $\ell$ doesn't divide the leading coefficient of $F$ or $G$; and,

(iii) For any $a, b \in \mathbb{Z}$ for which $F^aG^b$ is identically constant in $\overline{\mathbb{F}}_\ell(T)$, we have $\ell \mid a$ and $\ell \mid b$.

We will now show that any such constant $\kappa_1(F,G)$ satisfies the property in subpart (b) of the lemma. By subpart (a), $F(X)F(Y)F(Z)-u$ is already irreducible in $\overline{\mathbb{F}}_\ell[X,Y,Z]$ for any $u \in \mathbb{F}_\ell^\times$. Assume by way of contradiction that for some $\ell > \kappa_1(F,G)$ and $u, w \in \mathbb{F}_\ell^\times$, we have

$$G(X)G(Y)G(Z)-w = H_0(X,Y,Z)\,(F(X)F(Y)F(Z)-u) \text{ for some } H_0 \in \overline{\mathbb{F}}_\ell[X,Y,Z]. \tag{10.2}$$

Write $H_0(X,Y,Z) =: \sum_{\substack{0\leq i_1\leq r_1 \\ 0\leq i_2\leq r_2}} h_{i_1,i_2}(X)Y^{i_1}Z^{i_2}$ for some $h_{i_1,i_2} \in \overline{\mathbb{F}}_\ell[X]$ with $h_{r_1,r_2}$ not identically zero. If $(r_1,r_2) = (0,0)$, then substituting a root of $F$ and $G$ in place of $Y$ and $Z$ respectively, we see that $H_0$ must be a constant $\lambda_0 \in \overline{\mathbb{F}}_\ell\setminus\{0\}$ satisfying $w = \lambda_0 u$. Thus $G(X)G(Y)G(Z) = \lambda_0 F(X)F(Y)F(Z)$. Now substituting some $\eta \in \overline{\mathbb{F}}_\ell$ which is not a root of $FG$ in place of both $Y$ and $Z$ leads to $F(X)G(X)^{-1} = \lambda_0^{-1}F(\eta)^{-2}G(\eta)^2$, a nonzero constant. But since $(1,-1) \not\equiv (0,0) \pmod{\ell}$, this violates condition (iii) in the definition of $\kappa_1(F,G)$. Hence $(r_1,r_2) \neq (0,0)$.

[8] It is not difficult to see that this also forces $a = b = 0$, but we won't need that.

Let $\alpha, \beta \in \mathbb{Z}$ denote the leading coefficients of $F$ and $G$ respectively. Comparing the monomials in $Y$ and $Z$ of maximal total degree in (10.2) yields $\beta^2 G(X) = \alpha^2 F(X) h_{r_1,r_2}(X)$ in $\overline{\mathbb{F}}_\ell[X]$, so that (since either side of this identity is nonzero), we get $F \mid G$ in $\overline{\mathbb{F}}_\ell[X]$. Write $G = F^m H$ for some $m \geq 1$ and $H \in \overline{\mathbb{F}}_\ell[X]$ such that $F \nmid H$ in $\overline{\mathbb{F}}_\ell[X]$. An easy finite induction shows that with $G_t(X,Y,Z) \coloneqq F(X)^{m-t}F(Y)^{m-t}F(Z)^{m-t}H(X)H(Y)H(Z) - u^{-t}w$ and $\widehat{F}(X,Y,Z) \coloneqq F(X)F(Y)F(Z) - u$, we have $\widehat{F} \mid G_t$ for each $t \in \{0,1,\dots,m\}$. Indeed, the case $t = 0$ is just (10.2), and if $\widehat{F} \mid G_t$ for some $t \leq m-1$, then writing $G_t = Q_t \widehat{F}$ shows that $F(X)F(Y)F(Z) \mid (Q_t(X,Y,Z) - u^{-(t+1)}w)$. With $Q_{t+1}$ defined by $Q_t(X,Y,Z) - u^{-(t+1)}w = F(X)F(Y)F(Z)Q_{t+1}(X,Y,Z)$, we obtain $G_{t+1} = Q_{t+1}\widehat{F}$ completing the induction.

Applying this last observation with $t \coloneqq m$ shows that $\widehat{F}(X,Y,Z)$ divides $H(X)H(Y)H(Z) - u^{-m}w$ in $\overline{\mathbb{F}}_\ell[X,Y,Z]$. We claim that this forces $H$ to be constant. Indeed if not, then letting $\gamma \in \overline{\mathbb{F}}_\ell \setminus \{0\}$ be the leading coefficient of $H$, [9] writing $H(X)H(Y)H(Z) - u^{-m}w = (F(X)F(Y)F(Z) - u) \sum_{\substack{0 \leq i_1 \leq b_1 \\ 0 \leq i_2 \leq b_2}} g_{i_1,i_2}(X) Y^{i_1} Z^{i_2}$ for some $g_{i_1,i_2} \in \overline{\mathbb{F}}_\ell[X]$ with $g_{b_1,b_2} \neq 0$, and comparing the monomials in $Y$ and $Z$ of maximal degree, we obtain $\gamma^2 H(X) = \alpha^2 F(X) g_{b_1,b_2}(X)$. This leads to $F \mid H$, contrary to hypothesis. Hence $H$ must be constant, so the identity $F^{-m}G = H$ in $\overline{\mathbb{F}}_\ell(X)$ violates condition (iii) in the definition of $\kappa_1(F,G)$, as $(-m,1) \not\equiv (0,0) \pmod{\ell}$. This shows that $\widehat{F}$ cannot divide $G(X)G(Y)G(Z) - w$, completing the proof. □

Given a commutative ring $R$ and an $R$-module $M$, we say that $x \in R$ is an $M$-regular element if $x$ is not a zero-divisor on $M$, that is, if $xz = 0$ for some $z \in M$ implies $z = 0$. A sequence $x_1, \dots, x_n$ of elements of $R$ is said to be $M$-regular if $x_1$ is an $M$-regular element, each $x_i$ is an $M/(x_1,\dots,x_{i-1})M$-regular element, *and* $M/(x_1,\dots,x_n)M \neq 0$. It is well-known (see [5, Proposition 1.2.14]) that for any proper ideal $I$ in a Noetherian ring $R$, the height of $I$ is at least the length of the longest $R$-regular sequence contained in $I$.

*Proof of Proposition 10.1.* With $\kappa_0(F)$ and $\kappa_1(F,G)$ as in Lemma 10.3, the affine plane curve $\{(X,Y) \in \overline{\mathbb{F}}_\ell^2 : \ F(X)F(Y) - w = 0\}$ is absolutely irreducible for any $\ell > \kappa_0(F)$, so that Proposition 10.2(a) yields Proposition 10.1(a). For (b), it suffices to show that for any prime $\ell > \kappa_1(F,G)$, the variety $V_\ell \subset \overline{\mathbb{F}}_\ell^3$ defined by the polynomials $\widehat{F}(X,Y,Z) \coloneqq F(X)F(Y)F(Z) - u$ and $\widehat{G}(X,Y,Z) \coloneqq G(X)G(Y)G(Z) - w$ has $\ll_{F,G} \ell$ many $\mathbb{F}_\ell$-rational points. Consider the ideal $I(V_\ell)$ of the ring $R \coloneqq \overline{\mathbb{F}}_\ell[X,Y,Z]$ consisting of all polynomials vanishing at all the points of $V_\ell$, so that $(\widehat{F}, \widehat{G}) \subset I(V_\ell)$. If $I(V_\ell) = R$, then $V_\ell = \emptyset$, so suppose $I(V_\ell) \subsetneq R$. Lemma 10.3(b) shows that the sequence $\widehat{G}, \widehat{F} \in I(V_\ell)$ is $R$-regular, so by [5, Proposition 1.2.14], $I(V_\ell)$ has height at least 2. By [4, Chapter 11, Exercise 7], the Krull-dimension of $R$ is 3, whence that of $R/I(V_\ell)$ is at most $3 - 2 = 1$ (by, say, [24, p. 31]). Thus $\dim(V_\ell) \leq 1$, and Proposition 10.2 completes the proof. □

## 11. Restricted inputs to squarefree moduli: Proof of Theorem 2.3

Returning to the notation set up in the introduction, we start with the same initial reductions as in section 9. As such, to establish subpart (a) of the theorem, it suffices to show the bound

[9] Here $\gamma \neq 0$ in $\overline{\mathbb{F}}_\ell$ because $\ell$ doesn't divide the leading coefficient of $G = F^m H$.

(i) below with $k \geq 2$ and with the respective values of $R$ defined in the statement, – while in order to establish subpart (b), it suffices to show (ii) below, with the $2K+1$ replaced by 2 in the case when $K = 1$ and $W_k = W_{1,k}$ is not squarefull:

(11.1)

$$\text{(i) } \sideset{}{^*}\sum_{n:\ P_R(n)>q} 1 \ll \frac{x^{1/k}}{\varphi(q)^K (\log x)^{1-2\alpha_k/3}}, \text{ (ii) } \sideset{}{^*}\sum_{n:\ P_{2K+1}(n_k)>q} 1 \ll \frac{x^{1/k}}{\varphi(q)^K (\log x)^{1-2\alpha_k/3}}.$$

Here we again have $\epsilon = 1$ and $y = \exp(\sqrt{\log x})$ in the framework developed in section 4. We will also retain the notation $\omega_{\|}(n) = \#\{p > q : p^k \parallel n\} = \#\{n \leq x : p \parallel n_k\}$, $\omega^*(n) = \#\{p > q : p^{k+1} \mid n\}$, and $\omega_k(n) = \#\{p > q : p^2 \mid n_k\}$ from section 9.

For technical reasons, we first give a separate proof of all the above bounds in the case $K = 1$ (so that $f = f_1$). These bounds would follow once we show that

$$\sideset{}{^*}\sum_{n:\ P_{tk+1}(n)>q} 1 \ll \frac{x^{1/k}}{\varphi(q)(\log x)^{1-2\alpha_k/3}}, \tag{11.2}$$

with $t \coloneqq 1$ if $W_k$ is not squarefull, and with $t \coloneqq 2$ in general. Indeed any $n$ with $P_2(n_k) > q$ automatically has $P_{k+1}(n) \geq P_{2k}(n) > q$, and any $n$ with $P_3(n_k) > q$ automatically has $P_{2k+1}(n) \geq P_{3k}(n) > q$, so (11.1)(ii), as well as its analogue with $2K+1$ replaced by 2, would also follow once we show (11.2).

To show (11.2), we start by estimating the contribution of the $n$'s which are divisible by the $(k+1)$-th power of a prime exceeding $q$. Any such $n$ can be written in the form $mp^cP^k$ for some positive integers $m, c$ and primes $p, P$, satisfying $P = P(n) > z$, $q < p < P$, $c \geq k+1$, $P_{Jk}(m) \leq y$ and $f(n) = f(m)f(p^c)W_k(P)$. Recalling that $\#\{u \in U_q : W_k(u) \equiv b \pmod q\} \ll D^{\omega(q)}$ uniformly in $b \in \mathbb{Z}$, the argument given for the second bound in (9.4) shows that the contribution of such $n$ is $\ll \frac{D^{\omega(q)}}{q^{1/k}\varphi(q)} \cdot \frac{x^{1/k}}{(\log x)^{1-2\alpha_k/3}} \ll \frac{x^{1/k}}{\varphi(q)(\log x)^{1-2\alpha_k/3}}$. On the other hand, for any $n$ counted in (11.2) which is not divisible by the $(k+1)$-th power of any prime exceeding $q$, the condition $P_{tk+1}(n) > q$ forces $\omega_{\|}(n) \geq t+1$ (again since $q$ is sufficiently large and the $q$-rough part of $n$ is $k$-full). Thus $n = m(P_{t+1} \cdots P_1)^k$, for some $m$ and primes $P_1, \ldots, P_{t+1}$ satisfying $P_1 \coloneqq P(n) > z$, $q < P_{t+1} < \cdots < P_1$, $P_{Jk}(m) \leq y$ and $f(n) = f(m)\prod_{j=1}^{t+1} W_k(P_j)$. The arguments leading to (9.6) show that the contribution of such $n$ is

$$\ll \frac{V'_{t+1,1}}{\varphi(q)^{t+1}} \cdot \frac{x^{1/k}}{(\log x)^{1-\alpha_k/2}} \exp\left(O\big((\log_3 x)^2 + (\log_2(3q))^{O(1)}\big)\right). \tag{11.3}$$

Now when $W_k$ is not squarefull (so that $t+1 = 2$), Proposition 10.1(a) shows that $V'_{2,1}/\varphi(q)^2 \ll \varphi(q)^{-1}\exp(O(\sqrt{\log q}))$, inserting which into (11.3) yields (11.2). In general (when $t+1 = 3$), we may invoke (5.32) (with $K = L = 1$ and $G_{1,1} \coloneqq W_k = W_{1,k}$) to see that $V'_{3,1}/\varphi(q)^3 \ll \varphi(q)^{-1}\exp(O(\sqrt{\log q}))$, once again showing (11.2). This proves Theorem 2.3 for $K = 1$.

We may therefore assume in the rest of the proof that $K \geq 2$. By replicating the arguments given for the first two bounds in (9.4) (and replacing the use of Proposition 4.4 by Corollary 5.5), we arrive at the following analogous of these two bounds:

$$\sideset{}{^*}\sum_{n:\ \omega_{\|}(n)\geq 2K+1} 1, \sideset{}{^*}\sum_{\substack{n:\ \omega_{\|}(n)=2K \\ \omega^*(n)\geq 1}} 1 \ll \frac{x^{1/k}}{\varphi(q)^K(\log x)^{1-2\alpha_k/3}}, \tag{11.4}$$