Consider an arbitrary such tuple $(\tau_1, \dots, \tau_s)$, and write n in the form $mp_1^{c_1} \cdots p_s^{c_s} P_1^k \cdots P_r^k$ as above. The conditions $f_i(n) \equiv a_i \pmod q$ lead to $(P_1, \dots, P_r) \bmod q \in \mathcal{V}_{r,K}^{(k)}\big(q; (a_i f_i(mp_1^{c_1} \cdots p_s^{c_s})^{-1})_{i=1}^K\big)$. Given $m, p_1, \dots, p_s, c_1, \dots, c_s$ and $(v_1, \dots, v_r) \in \mathcal{V}_{r,K}^{(k)}\big(q; (a_i f_i(mp_1^{c_1} \cdots p_s^{c_s})^{-1})_{i=1}^K\big)$, the arguments leading to (9.5) show that the number of possible $P_1, \dots, P_r$ satisfying $P_j \equiv v_j \bmod q$ for each $j \in [r]$, is $\ll x^{1/k}(\log_2 x)^{O(1)}\big/\varphi(q)^r m^{1/k} p_1^{c_1/k} \cdots p_s^{c_s/k} \log x$. With $V'_{r,K} = \max_{(w_i)_i \in U_q^K} \#\mathcal{V}_{r,K}^{(k)}\big(q; (w_i)_{i=1}^K\big)$ as before, the bounds $\sum_{p_i > q:\ c_i \ge \tau_i} p_i^{-c_i/k} \ll q^{-(\tau_i/k-1)}$ yield

$$\mathcal{N}_{r,s}(\tau_1, \dots, \tau_s) \ll \frac{1}{q^{(\tau_1 + \dots + \tau_s)/k - s}} \frac{V'_{r,K}}{\varphi(q)^r} \cdot \frac{x^{1/k}(\log_2 x)^{O(1)}}{\log x} \sum_{\substack{m \le x:\ P(m) \le q \\ \gcd(f(m), q) = 1}} \frac{1}{m^{1/k}}. \tag{9.9}$$

Proceeding as in the argument for (4.5), we write any m in the above sum as BM where B is k-free and M is k-full, so that $B = O(1)$ and $P(M) \le q$. We find that

$$\sum_{\substack{m \le x:\ P(m) \le q \\ \gcd(f(m), q) = 1}} \frac{1}{m^{1/k}} \ll \sum_{\substack{M \le x:\ P(M) \le q \\ M \text{ is } k\text{-full}}} \frac{1}{M^{1/k}} \le \prod_{p \le q} \left(1 + \frac{1}{p} + O\left(\frac{1}{p^{1+1/k}}\right)\right) \ll \exp\left(\sum_{p \le q} \frac{1}{p}\right) \ll \log q. \tag{9.10}$$

Inserting this into (9.9), we obtain

$$\mathcal{N}_{r,s}(\tau_1, \dots, \tau_s) \ll \frac{1}{q^{(\tau_1 + \dots + \tau_s)/k - s}} \frac{V'_{r,K}}{\varphi(q)^r} \cdot \frac{x^{1/k}(\log_2 x)^{O(1)}}{\log x}. \tag{9.11}$$

Now since $1 \le r \le KD - 1$, an application of (4.10) with $N := r$ now yields

$$\mathcal{N}_{r,s}(\tau_1, \dots, \tau_s) \ll \frac{\exp\big(O(\omega(q))\big)}{q^{(\tau_1 + \dots + \tau_s)/k - s + r/D}} \cdot \frac{x^{1/k}(\log_2 x)^{O(1)}}{\log x} \ll \frac{\exp\big(O(\omega(q))\big)}{q^{\max\{s/k, R/k - r - s\} + r/D}} \cdot \frac{x^{1/k}(\log_2 x)^{O(1)}}{\log x}, \tag{9.12}$$

where in the last equality we have recalled that $\tau_1, \dots, \tau_s \ge k + 1$ and $\tau_1 + \dots + \tau_s \ge R - kr$. We claim that $\max\{s/k, R/k - r - s\} + r/D > K$. This is tautological if $s/k + r/D > K$, so suppose $s/k + r/D \le K$. Then $r \le D(K - s/k) \le DK - D/k$, and $s \le k(K - r/D)$ so that $R/k - r - s + r/D \ge R/k - Kk + ((k+1)/D - 1)r$. If $k < D$, then $(k+1)/D - 1 \le 0$, so for all $1 \le r \le DK - D/k$, we have $R/k - Kk + ((k+1)/D - 1)r \ge R/k - Kk + ((k+1)/D - 1)(DK - D/k)$ and this exceeds K since $R \ge k(KD + 1)$. If on the other hand, we had $k \ge D$, then $k + 1 > D$ and the minimum value of $R/k - Kk + ((k+1)/D - 1)r$ is attained at $r = 1$, giving us $R/k - Kk + ((k+1)/D - 1)r \ge R/k - Kk + ((k+1)/D - 1)$ which also exceeds K since $R > k\big(1 + (1 + k)(K - 1/D)\big)$. This shows our claim, so that (9.12) leads to (9.8). Summing (9.8) over the $O(1)$ many possible tuples $(\tau_1, \dots, \tau_s)$ occurring in the right hand side of (9.7) yields $\Sigma_{r,s} \ll x^{1/k}(\log_2 x)^{O(1)}\big/q^K \log x$, which (as argued before) establishes Theorem 2.2(a).

Completing the proof of Theorem 2.2(b): Define $\omega_k(n) := \#\{p > q : p^2 \mid n_k\}$. Any n with $\omega_k(n) = 0$ counted in (9.3)(ii) also has $\omega_\|(n) \ge KD + 1$ (since $P_{KD+1}(n_k) > q$), and hence any such n is counted in the first sum in (9.4). Likewise, any n with $\omega_\|(n) = KD$ counted in (9.3)(ii) has $\sum_{p > q:\ v_p(n_k) > 1} v_p(n_k) \ge (KD + 1) - \omega_\|(n) \ge 1$, so that any such n also has $\omega^*(n) \ge \omega_k(n) \ge 1$ and is counted in the second sum in (9.4). It thus remains to show that for each $r \in [KD - 1]$ and $s \in [Kk - 1]$, the contribution $\widetilde{\Sigma}_{r,s}$ of all n with $\omega_\|(n) = r$ and $\omega_k(n) = s$ to the left hand side of (9.3)(ii) is absorbed in the right.

Any n counted in $\widetilde{\Sigma}_{r,s}$ has n_k of the form $m'p_1^{c_1}\cdots p_s^{c_s}P_1\cdots P_r$ for some distinct primes $p_1,\dots,p_s$, $P_1,\dots,P_r$ and integers $m',c_1,\dots,c_s$, which satisfy conditions (i)–(v): **(i)** $P(m')\le q$; **(ii)** $P_1 := P(n_k) = P(n) > z$, $q < P_r < \cdots < P_1$; **(iii)** $p_1,\dots,p_s > q$; **(iv)** $c_1,\dots,c_s \ge 2$ and $c_1+\cdots+c_s \ge KD+1-r$; **(v)** m', $p_1,\dots,p_s,P_1,\dots,P_r$ are all pairwise coprime. Hence, n is of the form $mp_1^{c_1k}\cdots p_s^{c_sk}P_1^k\cdots P_r^k$, where $p_1,\dots,p_s,P_1,\dots,P_r$ are as above, and: **(vi)** $P_{Jk}(m)\le y$; **(vii)** $f_i(n) = f_i(m)f_i(p_1^{c_1k})\cdots f_i(p_s^{c_sk})\prod_{j=1}^r W_{i,k}(P_j)$ for each $i\in[K]$.

Now since $r \le KD-1$, the integers $\tau_j := \min\{c_j, KD+1-r\}$ ($j\in[s]$) satisfy $\tau_1,\dots,\tau_s \in [2, KD+1-r]$ and $\tau_1+\cdots+\tau_s \ge KD+1-r$. We now obtain the following analogue of (9.7)

$$\widetilde{\Sigma}_{r,s} \le \sum_{\substack{\tau_1,\dots,\tau_s\in[2,KD+1-r]\\ \tau_1+\cdots+\tau_s\ge KD+1-r}} \widetilde{\mathcal{N}}_{r,s}(\tau_1,\dots,\tau_s), \tag{9.13}$$

where $\widetilde{\mathcal{N}}_{r,s}(\tau_1,\dots,\tau_s)$ denotes the number of n which can be written in the form $mp_1^{c_1k}\cdots p_s^{c_sk}P_1^k\cdots P_r^k$ with $m,p_1,\dots,p_s,c_1,\dots,c_s,P_1,\dots,P_r$ satisfying the conditions (ii), (iii), (vi), (vii) above, and with $c_1\ge\tau_1,\dots,c_s\ge\tau_s$. We show that for each $\tau_1,\dots,\tau_s$ counted above,

$$\widetilde{\mathcal{N}}_{r,s}(\tau_1,\dots,\tau_s) \ll \frac{x^{1/k}}{\varphi(q)^K(\log x)^{1-2\alpha_k/3}}. \tag{9.14}$$

The argument is analogous to that given for (9.8), so we only sketch it. We write any n counted in $\widetilde{\Sigma}_{r,s}$ in the form $mp_1^{c_1k}\cdots p_s^{c_sk}P_1^k\cdots P_r^k$, with $m,p_1,\dots,p_s,c_1,\dots,c_s,P_1,\dots,P_r$ satisfying the conditions (ii), (iii), (vi), (vii) above, and with $c_1\ge\tau_1,\dots,c_s\ge\tau_s$, so that $(P_1,\dots,P_r) \bmod q \in \mathcal{V}_{r,K}^{(k)}\big(q;(a_if_i(mp_1^{c_1k}\cdots p_s^{c_sk})^{-1})_{i=1}^K\big)$. Thus, given $m,p_1,\dots,p_s,c_1,\dots,c_s$ and $(v_1,\dots,v_r)\in\mathcal{V}_{r,K}^{(k)}\big(q;(a_if_i(mp_1^{c_1k}\cdots p_s^{c_sk})^{-1})_{i=1}^K\big)$, the number of possible $P_1,\dots,P_r$ satisfying $P_j\equiv v_j \pmod q$ for each $j\in[r]$, is $\ll x^{1/k}(\log_2 x)^{O(1)}/\varphi(q)^r m^{1/k}p_1^{c_1}\cdots p_s^{c_s}\log x$. Hence

$$\widetilde{\mathcal{N}}_{r,s}(\tau_1,\dots,\tau_s) \ll \frac{1}{q^{\tau_1+\cdots+\tau_s-s}}\,\frac{V'_{r,K}}{\varphi(q)^r}\cdot\frac{x^{1/k}}{(\log x)^{1-\alpha_k/2}}\exp\left(O\left((\log_3 x)^2+(\log_2(3q))^{O(1)}\right)\right). \tag{9.15}$$

Now applying (4.10) and using the fact that $\tau_1+\cdots+\tau_s\ge\max\{2s,KD+1-r\}$, we find that $V'_{r,K}/\varphi(q)^rq^{\tau_1+\cdots+\tau_s-s} \ll \exp\big(O(\omega(q))\big)/q^{\max\{s,KD+1-r-s\}+r/D} \ll \varphi(q)^{-K}$, since from $D\ge 2$, it is easily seen that $\max\{s,KD+1-r-s\}+r/D > K$. This establishes (9.14), so that (9.13) yields $\widetilde{\Sigma}_{r,s} \ll x^{1/k}/\varphi(q)^K(\log x)^{1-2\alpha_k/3}$, completing the proof of Theorem 2.2(b). □

10. Final preparatory step for Theorem 2.3: Counting points on varieties

To establish Theorem 2.3, we will need the following partial improvements of Corollary 5.5. In this section, we again deviate from the general notation set up for Theorems 2.1 to 2.4, so the notation set up in this section will be relevant in this section only.

Proposition 10.1. *Let $F\in\mathbb{Z}[T]$ be a fixed nonconstant polynomial which is not squarefull.*

- **(a)** *Define $\mathcal{V}_{2,1}(\ell;w) := \{(v_1,v_2)\in U_\ell^2 : F(v_1)F(v_2)\equiv w \pmod \ell\}$. Then $\#\mathcal{V}_{2,1}(\ell;w) \le \varphi(\ell)\left(1+O\left(\ell^{-1/2}\right)\right)$, uniformly for primes ℓ and coprime residues w mod ℓ.*

- **(b)** *Let $G \in \mathbb{Z}[T]$ be any fixed polynomial such that $\{F, G\} \subset \mathbb{Z}[T]$ are multiplicatively independent. Let $\mathcal{V}_{3,2}(\ell; u, w)$ be the set of $(v_1, v_2, v_3) \in U_\ell^3$ satisfying the two congruences $F(v_1)F(v_2)F(v_3) \equiv u \pmod{\ell}$ and $G(v_1)G(v_2)G(v_3) \equiv w \pmod{\ell}$. Then $\#\mathcal{V}_{3,2}(\ell; u, w) \ll_{F,G} \varphi(\ell)$, uniformly in primes ℓ and coprime residues u, w mod ℓ.*

Our starting idea will be to look at $\mathcal{V}_{2,1}(\ell; w)$ and $\mathcal{V}_{3,2}(\ell; u, w)$ as subsets of the sets of $\mathbb{F}_\ell$-rational points of certain varieties over the algebraic closure $\overline{\mathbb{F}}_\ell$ of $\mathbb{F}_\ell$.

Proposition 10.2. *Let V be a variety defined over $\mathbb{F}_\ell$ and $V(\mathbb{F}_\ell) := V \cap \mathbb{F}_\ell$.*

- **(a)** *If V is an absolutely irreducible affine plane curve, then $\#V(\mathbb{F}_\ell) \le \ell + O(\sqrt{\ell})$, where the implied constant depends only on the degree of V.*
- **(b)** *Let d be the positive integer such that $V \subset (\overline{\mathbb{F}}_\ell)^d$. We have $\#V(\mathbb{F}_\ell) \ll \ell^{\dim V}$, where $\dim V$ is the dimension of V as a variety, and the implied constant depends at most on d and on the number and degrees of the polynomials defining V.*

Subpart(a) is a consequence of [23, Corollary 2b], while subpart (b) is a weaker version of [12, Claim 7.2] but in fact goes back to work of Lang and Weil [21, Lemma 1]. To make use of the aforementioned results, we will also be needing the following observations.

Lemma 10.3. *Let $F, G \in \mathbb{Z}[T]$ be fixed multiplicatively independent polynomials such that F is not squarefull. There exist constants $\kappa_0(F)$ and $\kappa_1(F, G)$ such that:*

- **(a)** *For any $N \ge 2$, $\ell > \kappa_0(F)$ and $w \in \mathbb{F}_\ell^\times$, the polynomial $\prod_{i=1}^N F(X_i) - w$ is absolutely irreducible over $\mathbb{F}_\ell$, that is, it is irreducible in the ring $\overline{\mathbb{F}}_\ell[X_1, \dots, X_N]$.*
- **(b)** *For any $\ell > \kappa_1(F, G)$ and $u, w \in \mathbb{F}_\ell^\times$, the polynomial $F(X)F(Y)F(Z) - u$ is irreducible and doesn't divide the polynomial $G(X)G(Y)G(Z) - w$ in the ring $\overline{\mathbb{F}}_\ell[X, Y, Z]$.*

Proof. Write $F := r \prod_{j=1}^M G_j^{b_j}$ for some $r \in \mathbb{Z}$, $b_j \in \mathbb{N}$, and pairwise coprime irreducibles $G_j \in \mathbb{Z}[T]$, so that by the nonsquarefullness of F in $\mathbb{Z}[T]$, we have $b_j = 1$ for some $j \in [M]$. By the observations at the start of the proof of Proposition 5.3, there exists a constant $\kappa_0(F)$ such that for any prime $\ell > \kappa_0(F)$, ℓ doesn't divide the leading coefficient of F and $\prod_{j=1}^M G_j$ is separable in $\mathbb{F}_\ell[T]$. This forces $\prod_{\substack{\theta \in \overline{\mathbb{F}}_\ell \\ F(\theta)=0}} (T - \theta)^2 \nmid F(T)$ in $\overline{\mathbb{F}}_\ell[T]$.

Proof of (a). We will show that for any $\ell > \kappa_0(F)$ and $U, V \in \overline{\mathbb{F}}_\ell[X_1, \dots, X_N]$ satisfying

$$\prod_{i=1}^N F(X_i) - w = U(X_1, \dots, X_N)V(X_1, \dots, X_N), \tag{10.1}$$

one of U or V must be constant. First note that for any root $\theta \in \overline{\mathbb{F}}_\ell$ of F, we have $-w = U(X_1, \dots, X_{N-1}, \theta)V(X_1, \dots, X_{N-1}, \theta)$, forcing $U(X_1, \dots, X_{N-1}, \theta)$ and $V(X_1, \dots, X_{N-1}, \theta)$ to be constant in the ring $\overline{\mathbb{F}}_\ell[X_1, \dots, X_N]$. Writing $U(X_1, \dots, X_N)$, $V(X_1, \dots, X_N)$ as

$$\sum_{\substack{i_1, \dots, i_{N-1} \ge 0 \\ i_1 \le R_1, \dots, i_{N-1} \le R_{N-1}}} u_{i_1, \dots, i_{N-1}}(X_N)\ X_1^{i_1} \cdots X_{N-1}^{i_{N-1}}, \qquad \sum_{\substack{j_1, \dots, j_{N-1} \ge 0 \\ j_1 \le T_1, \dots, j_{N-1} \le T_{N-1}}} v_{j_1, \dots, j_{N-1}}(X_N)\ X_1^{j_1} \cdots X_{N-1}^{j_{N-1}}$$