Chapter 12

Sieve Methods

12.1. The sieve of Eratosthenes

The Inclusion-Exclusion principle, or the Möbius inversion formula, can be used—at least theoretically—to calculate $\pi(x)$. For a sufficiently large x, let us write

$$P = \prod_{p \le \sqrt{x}} p.$$

Then an integer n with $\sqrt{x} < n < x$ is prime if and only if $(n, P) = 1$. Thus, we can write

$$\begin{aligned} \pi(x) - \pi(\sqrt{x}) + 1 &= \sum_{n \le x} E((n, P))) = \sum_{n \le x} \sum_{\substack{d \mid n \\ d \mid P}} \mu(d) \\ &= \sum_{d \mid P} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor, \end{aligned} \tag{12.1}$$

where, as we have seen,

$$E(n) = \sum_{d \mid n} \mu(d)$$

is 1 if $n = 1$ and 0 otherwise (see Theorem 4.8(i)). If at this stage we insert the simple estimate

$$\left\lfloor \frac{x}{d} \right\rfloor = \frac{x}{d} + O(1)$$

in (12.1), we obtain

$$\pi(x) - \pi(\sqrt{x}) + 1 = x \prod_{p \le \sqrt{x}} \left(1 - \frac{1}{p}\right) + O(2^{\pi(\sqrt{x})}). \tag{12.2}$$

By the estimate of Problem 4.4, the first term of the right-hand side of (12.2) is

$$\sim 2e^{-\gamma}\frac{x}{\log x} \qquad \text{as } x \to \infty,$$

while by Chebyshev's estimates, the error term in (12.2) can be seen to be larger than any power of x, thus showing that the error term in (12.2) can in fact be larger than the main term, thereby spoiling our goal of obtaining something worthwhile by this approach.

The above calls for two comments. On the one hand, the exact formula (12.1)—called the *sieve formula of Eratosthenes* or at times the *Legendre formula*—involves too many terms for any reasonable practical estimate. On the other hand, the estimate of the main term itself shows, taking into account the Prime Number Theorem and the fact that $e^{-\gamma} \neq 1$, that the "error terms" created by replacing $\lfloor x/d \rfloor$ by x/d have made a global contribution of the same order of magnitude as the "main term". This suggests that this method, even suitably adapted, will never allow for a proof of the Prime Number Theorem. However, it can provide Chebyshev type estimates in a wide context.

In order to obtain a nontrivial result starting from formula (12.1), one may introduce a parameter y, $2 \le y \le x$, and bound $\pi(x) - \pi(y) + 1$ by the number of integers $n \le x$ having no prime factor $p \le y$. With the same calculations we get

$$\begin{aligned} \pi(x) &\le x \prod_{p \le y} \left(1 - \frac{1}{p}\right) + O(2^y) \\ &= \frac{x(e^{-\gamma} + o(1))}{\log y} + O(2^y) \ll \frac{x}{\log\log x}, \end{aligned} \tag{12.3}$$

where we chose $y = \log x$.

With the aim of improving the efficiency of the above method, Viggo Brun invented the combinatorial sieve between 1917 and 1924.

12.2. The Brun sieve

The Eratosthenes sieve rests on the identity

$$\mu * \mathbf{1} = E.$$

Brun's idea was to introduce two auxiliary functions μ_1 and μ_2 satisfying

$$\mu_1 * \mathbf{1} \le E \le \mu_2 * \mathbf{1} \tag{12.4}$$

and vanishing often enough so that the number of nonzero terms in the resulting formula analogous with (12.1) is not overwhelming. Brun's initial choice led to what is now called *Brun's pure sieve* and is the following.

Theorem 12.1. *Denote by χ_t the characteristic function of the set of integers n such that $\omega(n) \le t$. Then for each integer $h \ge 0$, the functions defined by*

$$\mu_i(n) = \mu(n)\chi_{2h+2-i}(n) \qquad (i = 1, 2)$$

satisfy inequalities (12.4).

Proof. Since $\mu_i * 1(n)$ depends only on the kernel of n, we may assume that $\mu(n) \neq 0$. If $\omega(n) = k$, then, for each r with $0 \le r \le k$, it is clear that n has exactly $\binom{k}{r}$ divisors d with $\omega(d) = r$. For any given $t \ge 0$, we can thus write

$$\chi_t * 1(n) = \sum_{\substack{d \mid n \\ \omega(d) \le t}} \mu(d) = \sum_{0 \le r \le t} (-1)^r \binom{k}{r} = (-1)^t \binom{k-1}{t},$$

where the last equality is easily obtained by induction over t. □

The above result immediately yields the following corollary.

Corollary 12.2. *Let $\mathcal{A}$ be a finite set of integers and let $\mathcal{P}$ be a set of prime numbers. Write*

$$\begin{aligned} \mathcal{A}_d &= \#\{a \in \mathcal{A} : a \equiv 0 \pmod{d}\}, \\ P(y) &= \prod_{\substack{p \le y \\ p \in \mathcal{P}}} p, \\ \mathcal{S}(\mathcal{A}, \mathcal{P}, y) &= \#\{a \in \mathcal{A} : (a, P(y)) = 1\}. \end{aligned}$$

Then, for each integer $h \ge 0$,

$$\sum_{\substack{d \mid P(y) \\ \omega(d) \le 2h+1}} \mu(d)\mathcal{A}_d \le \mathcal{S}(\mathcal{A}, \mathcal{P}, y) \le \sum_{\substack{d \mid P(y) \\ \omega(d) \le 2h}} \mu(d)\mathcal{A}_d.$$

Let us see how the above result helps us to considerably improve the upper bound of $\pi(x)$ obtained by the Eratosthenes sieve (see (12.3)).

In Corollary 12.2, we chose $\mathcal{A} = \{n : n \le x\}$, $\mathcal{P} = \{\text{all primes}\}$ and $P = P(y) = \prod_{p \le y} p$. Then $\mathcal{S}(\mathcal{A}, \mathcal{P}, y)$ is the number of positive integers

$n \le x$ having no prime factor $p \le y$, so that

$$\begin{aligned}\mathcal{S}(\mathcal{A},\mathcal{P},y) &\le \sum_{\substack{d\mid P(y)\\ \omega(d)\le 2h}} \mu(d)\left\lfloor \frac{x}{d}\right\rfloor \\ &= x\sum_{\substack{d\mid P(y)\\ \omega(d)\le 2h}} \frac{\mu(d)}{d} + O\left(\sum_{\substack{d\mid P(y)\\ \omega(d)\le 2h}} 1\right) \qquad (12.5)\\ &= x\prod_{p\le y}\left(1-\frac{1}{p}\right) + O\left(\sum_{\substack{d\mid P(y)\\ \omega(d)\le 2h}} 1 + x\sum_{\substack{d\mid P(y)\\ \omega(d)> 2h}}\frac{1}{d}\right),\end{aligned}$$

and similarly

$$\begin{aligned}\mathcal{S}(\mathcal{A},\mathcal{P},y) &\ge \sum_{\substack{d\mid P(y)\\ \omega(d)\le 2h+1}} \mu(d)\left\lfloor \frac{x}{d}\right\rfloor \\ &= x\prod_{p\le y}\left(1-\frac{1}{p}\right) + O\left(\sum_{\substack{d\mid P(y)\\ \omega(d)\le 2h+1}} 1 + x\sum_{\substack{d\mid P(y)\\ \omega(d)> 2h+1}}\frac{1}{d}\right). \qquad (12.6)\end{aligned}$$

The first of the two error terms appearing either at (12.5) or at (12.6) does not exceed y^{2h+1} since this is an upper bound for all integers d such that $d \mid P(y)$ and $\omega(d) \le 2h+1$. The d-sums arising in the second error terms are bounded, in light of the arguments already used in Chapter 11, namely, for example, for the second error term in (12.5), by

$$\sum_{\substack{d\mid P(y)\\ \omega(d)>2h}} \frac{1}{d} \le \sum_{k>2h}\frac{1}{k!}\left(\sum_{p\le y}\frac{1}{p}\right)^k \le \sum_{k>2h}\frac{1}{k!}(\log\log y + c_0)^k.$$

Using the weak form of Stirling's formula (see 1.12), together with $y < x$, we get

$$\sum_{\substack{d\mid P(y)\\ \omega(d)>2h}} \frac{1}{d} \le \sum_{k>2h}\frac{1}{k!}\left(\log\log x + c_0\right)^k \le \sum_{k>2h}\left(\frac{e\log\log x + ec_0}{k}\right)^k.$$

Choosing the smallest integer $h \ge e\log\log x + ec_0$, we obtain

$$\sum_{\substack{d\mid P(y)\\ \omega(d)>2h}} \frac{1}{d} \le \left(\frac{1}{2}\right)^{2h}\left(1+\frac{1}{2}+\frac{1}{4}+\cdots\right) \ll \frac{1}{(\log x)^{2e\log 2}} \ll \frac{1}{(\log x)^2},$$

because $2e\log 2 = e\log 4 > e > 2$. For this choice of h, we impose that $y^{2h+1} \le x/(\log x)^2$, which for $h > 1$ is implied by

$$y \le \frac{x^{1/(2h+1)}}{\log x} \le \exp\left(\frac{\log x}{2e\log\log x + c_1} - \log\log x\right),$$

where we can take $c_1 = 2ec_0 + 1$. Since $1/2e > 1/10$, it follows that we may choose

$$y = \exp\left(\frac{\log x}{10\log\log x}\right), \tag{12.7}$$

in which case the inequality $y^{2h+1} \ll x/(\log x)^2$ holds for all x. With this choice of y, we have that

$$\prod_{p\le y}\left(1-\frac{1}{p}\right) \asymp \frac{1}{\log y} \asymp \frac{\log\log x}{\log x},$$

while the error terms in (12.5) and (12.6) are $O(x/(\log x)^2)$. Thus, we have proved that

$$\mathcal{S}(\mathcal{A},\mathcal{P},y) = x\prod_{p\le y}\left(1-\frac{1}{p}\right)\left(1+O\left(\frac{1}{\log y}\right)\right). \tag{12.8}$$

Since

$$\mathcal{S}(\mathcal{A},\mathcal{P},y) \ge \pi(x) - \pi(y) \ge \pi(x) - y \ge \pi(x) + O(x^{1/2}),$$

we immediately deduce that

$$\pi(x) \ll x^{1/2} + x\prod_{p\le y}\left(1-\frac{1}{p}\right) \ll \frac{x\log\log x}{\log x},$$

which, although much weaker than Chebyshev's estimate, is remarkable because of the simplicity and generality of the argument.

To summarize, we have just proved a result announced earlier (see (9.7)):

Theorem 12.3. *Letting*

$$\Phi(x,y) = \#\{n \le x : p(n) > y\},$$

then, for $y \le \exp\left(\dfrac{\log x}{10\log\log x}\right)$,

$$\Phi(x,y) = x\prod_{p\le y}\left(1-\frac{1}{p}\right)\left\{1+O\left(\frac{1}{\log y}\right)\right\}.$$

12.3. Twin primes

Now we expose another remarkable application of Brun's pure sieve, namely, the fact that the sum of the reciprocal of the twin primes is convergent.

Proposition 12.4. *Let* $\mathcal{J} = \{p : \ p \text{ and } p+2 \text{ are both primes}\}$ *and set* $\mathcal{J}(x) = \#\{p \le x : p \in \mathcal{J}\}$. *Then*

$$\mathcal{J}(x) \ll \frac{x(\log\log x)^2}{(\log x)^2}.$$

Proof. In Corollary 12.2, set $\mathcal{A} = \{n(n+2) : n \le x\}$. Again, let $\mathcal{P}$ stand for the set of all primes and let y be a parameter to be chosen later. To understand $\#\mathcal{A}_d$, we look at

$$\rho(d) = \#\{0 \le n \le d-1 \ : \ n(n+2) \equiv 0 \pmod d\}.$$

Let us first show that $\rho(d)$ is multiplicative. Indeed, if u and v are coprime and $c \pmod{uv}$ is some congruence class modulo uv such that $n(n+2) \equiv 0 \pmod{uv}$, then certainly $c \pmod u$ ($c \pmod v$, respectively) is a congruence class modulo u (modulo v, respectively) such that $n(n+2) \equiv 0 \pmod u$ ($n(n+2) \equiv 0 \pmod v$, respectively). Conversely, if $a \pmod u$ and $b \pmod v$ are congruence classes for n modulo u and v which are solutions to $n(n+2) \equiv 0 \pmod u$ and $n(n+2) \equiv 0 \pmod v$, respectively, then by the Chinese Remainder Theorem, there exists a class $c \pmod{uv}$ (which is unique) such that $c \equiv a \pmod u$ and $c \equiv b \pmod v$. Hence, $n(n+2) \equiv 0 \pmod u$ and $n(n+2) \equiv 0 \pmod v$, and since u and v are coprime, we get that $n(n+2) \equiv 0 \pmod{uv}$. This shows that $\rho(uv) = \rho(u)\rho(v)$. Note that $\rho(2) = 1,\ \rho(4) = 2,\ \rho(2^k) = 4$ for $k \ge 3$ and $\rho(p^k) = 2$ if $p > 2$ is odd. In particular, if d is squarefree, then $\rho(d) = 2^{\omega(d)}$ if d is odd and $\rho(d) = 2^{\omega(d)-1}$ if d is even. Since there are precisely $\rho(d)$ solutions n to the congruence $n(n+2) \equiv 0 \pmod d$ in any interval of length d, and since the interval $[1, x]$ is made up of $\lfloor x/d \rfloor$ intervals of length d and (maybe) one shorter interval, we get that

$$\begin{aligned} \mathcal{A}_d &= \#\{n \le x \ : \ d \mid n(n+2)\} = \rho(d)\left(\left\lfloor \frac{x}{d} \right\rfloor + O(1)\right) \\ &= \frac{x\rho(d)}{d} + O(\rho(d)) = \frac{x\rho(d)}{d} + O(2^{\omega(d)}). \end{aligned}$$

Upon noting that if $p, p+2$ are twin primes, then either $p \le y$ or $p \in \mathcal{S}(\mathcal{A}, \mathcal{P}, y)$, we have, by Corollary 12.2, that

(12.9)

$$\begin{aligned}
\mathcal{J}(x) &\le \pi(y) + \sum_{\substack{d \mid P(y) \\ \omega(d) \le 2h}} \mu(d)\mathcal{A}_d \\
&= \sum_{\substack{d \mid P(y) \\ \omega(d) \le 2h}} \mu(d) \left(\frac{x\rho(d)}{d} + O(2^{\omega(d)}) \right) + O(y) \\
&= x \sum_{\substack{d \mid P(y) \\ \omega(d) \le 2h}} \frac{\mu(d)\rho(d)}{d} + O\left(y + \sum_{\substack{d \mid P(y) \\ \omega(d) \le 2h}} 2^{\omega(d)} \right) \\
&= x \sum_{d \mid P(y)} \frac{\mu(d)\rho(d)}{d} + O\left(y + 2^{2h} \sum_{\substack{d \mid P(y) \\ \omega(d) \le 2h}} 1 + x \sum_{\substack{d \mid P(y) \\ \omega(d) > 2h}} \frac{2^{\omega(d)}}{d} \right) \\
&= x \prod_{p \le y} \left(1 - \frac{\rho(p)}{p} \right) + O\left(y + 2^{2h} \sum_{\substack{d \mid P(y) \\ \omega(d) \le 2h}} 1 + x \sum_{\substack{d \mid P(y) \\ \omega(d) > 2h}} \frac{2^{\omega(d)}}{d} \right) \\
&= \frac{x}{2} \prod_{3 \le p \le y} \left(1 - \frac{2}{p} \right) + O\left(y + (2y)^{2h} + x \sum_{\substack{d \mid P(y) \\ \omega(d) > 2h}} \frac{2^{\omega(d)}}{d} \right).
\end{aligned}$$

Using the combinatorial fact that

$$\sum_{\substack{d \mid P(y) \\ \omega(d) > 2h}} \frac{2^{\omega(d)}}{d} \le \sum_{k > 2h} \sum_{\substack{d \mid P(y) \\ \omega(d) = k}} \frac{2^k}{d} \le \sum_{k > 2h} \frac{1}{k!} \left(\sum_{p \le y} \frac{2}{p} \right)^k,$$

together with Mertens' formula and estimate (1.12), we get

$$\sum_{\substack{d \mid P(y) \\ \omega(d) > 2h}} \frac{2^{\omega(d)}}{d} < \sum_{k > 2h} \frac{1}{k!} (2 \log\log x + 2c_0)^k < \sum_{k > 2h} \left(\frac{2e \log\log x + c_1}{k} \right)^k,$$

where $c_1 = 2ec_0$. Hence, we see that if we choose h to be twice as large as in the proof of Theorem 12.3, that is, the minimal positive integer h larger

than $2e\log\log x + c_1$, we then get

$$\sum_{\substack{d\,|\,P(y)\\ \omega(d)>2h}} \frac{2^{\omega(d)}}{d} < \frac{1}{2^{2h}}\left(\sum_{l\ge 0}\frac{1}{2^l}\right) = \frac{2}{2^{2h}} \ll \frac{1}{(\log x)^{4e\log 2}} < \frac{1}{(\log x)^2}. \tag{12.10}$$

Choosing $y = \exp(\log x/(20\log\log x))$, we obtain that

$$(2y)^{2h} = 2^{2h}\exp\left(\frac{2h\log x}{20\log\log x}\right) = \exp\left(\frac{(1+o(1))4e\log x}{20}\right) \ll \frac{x}{(\log x)^2}. \tag{12.11}$$

Inserting estimates (12.10) and (12.11) into (12.9), we get

$$\mathcal{J}(x) \ll x\prod_{3\le p\le y}\left(1-\frac{2}{p}\right) + \frac{x}{(\log x)^2}.$$

Finally, using Problem 4.6 with $\kappa = -2$, we have that

$$\begin{aligned}\prod_{3\le p\le y}\left(1-\frac{2}{p}\right) &= \frac{c_2}{(\log y)^2}(1+o(1)) = c_2\left(\frac{20\log\log x}{\log x}\right)^2(1+o(1))\\ &= (1+o(1))\frac{400c_2(\log\log x)^2}{(\log x)^2},\end{aligned}$$

so that

$$\mathcal{J}(x) \ll \frac{x(\log\log x)^2}{(\log x)^2},$$

which is what we wanted to prove. □

Corollary 12.5. *The series*

$$\sum_{p,\ p+2\ \text{primes}}\frac{1}{p} < \infty.$$

Proof. Since

$$\mathcal{J}(n) - \mathcal{J}(n-1) = \begin{cases} 1 & \text{if } n \text{ and } n+2 \text{ are both primes,}\\ 0 & \text{otherwise,}\end{cases}$$

then, in light of Proposition 12.4,

$$\begin{aligned}\sum_{p,p+2\ \text{primes}}\frac{1}{p} &= \sum_{n=2}^{\infty}\frac{\mathcal{J}(n)-\mathcal{J}(n-1)}{n} = \sum_{n=1}^{\infty}\mathcal{J}(n)\left(\frac{1}{n}-\frac{1}{n+1}\right)\\ &= \sum_{n=1}^{\infty}\frac{\mathcal{J}(n)}{n(n+1)} \ll \sum_{n\ge e}\frac{n(\log\log n)^2}{(\log^2 n)\,n(n+1)}\\ &< \sum_{n\ge e}\frac{(\log\log n)^2}{n(\log n)^2} \ll \int_e^{\infty}\frac{(\log\log t)^2}{t\log^2 t}\,dt < \infty,\end{aligned}$$

as requested. □

12.4. The Brun combinatorial sieve

The theory described in the previous sections of this chapter was later refined by partitioning the interval $[1, y]$ into suitable subintervals $[y_j, y_{j+1}]$, where $1 = y_0 < y_1 < \cdots < y_k = y$ and selecting for $i = 1,\ 2$, $\mu_i(d) = \mu(d)\chi_i^*(d)$, where $\chi_i^*(d)$ is the characteristic function of the set of those positive integers n having exactly $2h_j+2-i$ prime factors in $[y_j, y_{j+1})$ for $j = 0,\ 1,\ \ldots,\ k-1$. We shall not provide any proof, but we will nevertheless state some of the basic results of the theory, which is known as the *Brun combinatorial sieve* or sometimes simply as the *Brun sieve*.

Theorem 12.6. *With the notations of Corollary* 12.2*, assume that there exists a nonnegative multiplicative function w, some real number X and positive constants κ and A such that*

$$\text{(i)}\ \ \mathcal{A}_d = X\frac{w(d)}{d} + R_d \qquad (d \mid P(y)),$$

$$\text{(ii)}\ \ \prod_{\eta\le p\le\zeta}\left(1-\frac{w(p)}{p}\right)^{-1} < \left(\frac{\log\zeta}{\log\eta}\right)^{\kappa}\left(1+\frac{A}{\log\eta}\right) \qquad (2\le\eta\le\zeta).$$

Then, uniformly for $\mathcal{A}, X, y, u \ge 1$,

$$\text{(12.12)}\ \ \mathcal{S}(\mathcal{A},\mathcal{P},y) = X\prod_{\substack{p\le y\\ p\in\mathcal{P}}}\left(1-\frac{w(p)}{p}\right)\{1+O(u^{-u/2})\}+O\left(\sum_{\substack{d\le y^u\\ d\mid P(y)}}|R_d|\right).$$

In the rest of this chapter, we shall give several applications of Theorem 12.6.

12.5. A Chebyshev type estimate

Choose $\mathcal{A} = \{n \le x\}$, $\mathcal{P}$ to be the set of all primes and $X = x$. Then (i) of Theorem 12.6 holds with $w(d) = 1$ for all $d \mid P(y)$ and $|R_d| \le 1$. To see that (ii) holds, use the fact that

$$\prod_{p\le z}\left(1-\frac{1}{p}\right) = \frac{c}{\log z}\left(1+O\left(\frac{1}{\log z}\right)\right)$$

for some constant $c > 0$ with $z = \eta$ and then with $z = \zeta$ and divide the two resulting relations to get that

(12.13)

$$\begin{aligned}\prod_{\eta\le p\le\zeta}\left(1-\frac{w(p)}{p}\right)^{-1} &= \prod_{\eta\le p\le\zeta}\left(1-\frac{1}{p}\right)^{-1}\\ &= \frac{(c/\log\eta)^{-1}}{(c/\log\zeta)^{-1}}\left(1+O\left(\frac{1}{\log\eta}\right)\right)^{-1}\left(1+O\left(\frac{1}{\log\zeta}\right)\right)\\ &= \frac{\log\zeta}{\log\eta}\left(1+O\left(\frac{1}{\log\eta}\right)\right)\left(1+O\left(\frac{1}{\log\zeta}\right)\right)\\ &= \frac{\log\zeta}{\log\eta}\left(1+O\left(\frac{1}{\log\eta}+\frac{1}{\log\zeta}\right)\right)\\ &= \frac{\log\zeta}{\log\eta}\left(1+O\left(\frac{1}{\log\eta}\right)\right),\end{aligned}$$

so that condition (ii) holds for some $A > 0$ with $\kappa = 1$. Now let c_1 be the constant implied by the O in (12.12) and let $u > 0$ be a constant such that $u^{u/2} > 2c_1$. Then the quantity $O(u^{-u/2})$ in (12.12) is in absolute value at most $c_1/u^{u/2} < 1/2$, so that the main term in (12.12) is $> \frac{x}{2}\prod_{p\le y, p\in\mathcal{P}}(1 - 1/p)$. Now choose y such that $y^u \le x^{1/2}$. Clearly, we may choose $y = x^{1/2u}$. Then the error term is $\ll y^u \le x^{1/2}$, and so we get that

$$\mathcal{S}(\mathcal{A},\mathcal{P},y) = x\prod_{p\le x^{1/2u}}\left(1-\frac{1}{p}\right)+O(x^{1/2}).$$

Since

$$\prod_{p\le x^{1/2u}}\left(1-\frac{1}{p}\right) = \frac{c}{\log(x^{1/2u})}\left(1+O\left(\frac{1}{\log(x^{1/2u})}\right)\right) = \frac{2cu}{\log x}(1+o(1))$$

as $x \to \infty$ and since u is a constant, we get, in particular, that

$$\pi(x) \le \pi(y) + \mathcal{S}(\mathcal{A},\ \mathcal{P}, y) \ll \frac{x}{\log x},$$

a Chebyshev type estimate (see Section 2.6 in Chapter 2).

12.6. The Brun-Titchmarsh theorem

Let $1 \le a < b$ be integers with $(a, b) = 1$. Let $\pi(x; b, a) = \#\{p \le x : p \equiv a \pmod b\}$. The following inequality is known as the *Brun-Titchmarsh inequality* or at times as the *Brun-Titchmarsh theorem.*

Theorem 12.7. *The inequality*

$$\pi(x; b, a) - \pi(x - z; b, a) \ll \frac{z}{\phi(b)\log(z/b)}$$

holds uniformly for $1 \le b < z \le x$ *and* $1 \le a < b$ *such that* $(a,b) = 1$. *The implied constant in the above* $\ll$ *symbol is absolute.*

Proof. We choose $\mathcal{A} = \{bm + a \in [x-z, x]\}$. We note that the numbers in $\mathcal{A}$ are always coprime with the primes $p \mid b$. We let $\mathcal{P} = \{p \le y : \ p \nmid b\}$, where $y < z$ will be chosen later. Since $x - z > 0$, it follows that any number $m \in [x-z, x]$ which is congruent to $a \pmod b$ is in $\mathcal{A}$, and if it is prime then it is coprime with all the primes $p \in \mathcal{P}$. Note that if $q \in \mathcal{P}$, then there is only one number $m \in \{0, 1, \dots, q-1\}$ such that $bm + a \equiv 0 \pmod q$. (This m is the congruence class of $-ab^{-1} \pmod q$.) Thus, $w(d) = 1$ if $d \mid P(y)$. Furthermore, if d is coprime to m and $d \mid bm + a$, then $m = m_0 + d\ell$, where $m_0 \in \{0, 1, \dots, d-1\}$ is the smallest nonnegative solution of the congruence $bm + a \equiv 0 \pmod d$. Thus, $bm + d = bd\ell + (bm_0 + a)$. The number of such numbers which are also in the interval $[x-z, x]$ is $\lfloor z/bd \rfloor + O(1)$. Hence, by applying Theorem 12.6(i),

$$\mathcal{A}_d = \frac{z}{b}\frac{w(d)}{d} + R_d,$$

where $|R_d| \le 1$ and this is true for all $d \mid P(y)$. Thus, we may choose $X = z/b$. Clearly,

$$\begin{aligned}\prod_{\substack{\eta \le p \le \zeta \\ p \in \overline{\mathcal{P}}}} \left(1 - \frac{w(p)}{p}\right)^{-1} &= \prod_{\substack{\eta \le p \le \zeta \\ p \nmid b}} \left(1 - \frac{1}{p}\right)^{-1} \le \prod_{\eta \le p \le \zeta} \left(1 - \frac{1}{p}\right)^{-1} \\ &\le \frac{\log \zeta}{\log \eta}\left(1 + O\left(\frac{1}{\log \eta}\right)\right),\end{aligned}$$

where the last inequality follows from (12.13). Thus, we may apply Theorem 12.6. Again, we choose some sufficiently large u such that the expression $1 + O(u^{-u/2})$ is in $(1/2, 3/2)$. Fixing the value of u in this range, we choose y such that $y^u \le X^{1/2}$. This means that we may choose $y = X^{1/(2u)} = (z/b)^{1/2u}$. With these choices, the error term in Theorem 12.6 is $\ll X^{1/2} \ll (z/b)^{1/2}$, while the main term is

$$\begin{aligned}\mathcal{S}(\mathcal{A}, \mathcal{P}, y) &\ll X \prod_{p \in \mathcal{P}(y)} \left(1 - \frac{1}{p}\right) \\ &= \frac{z}{b} \prod_{p \le y} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \le y \\ p \mid b}} \left(1 - \frac{1}{p}\right)^{-1} \\ &\ll \frac{z}{b}\frac{b}{\phi(b)}\frac{1}{\log y} = \frac{z}{\phi(b)}\frac{2u}{\log(z/b)} \\ &\ll \frac{z}{\phi(b)\log(z/b)}.\end{aligned}$$

To summarize,

$$\pi(x;b,a) - \pi(x-z;b,a) \ll \frac{z}{\phi(b)\log(z/b)} + \Big(\frac{z}{b}\Big)^{1/2}.$$

Let c_0 be such that $t^{1/2} > \log t$ for $t > c_0$. If $z/b > c_0$, then, since $\phi(b) \le b$, we have

$$\frac{z}{\phi(b)\log(z/b)} \ge \frac{z}{b\log(z/b)} \ge \Big(\frac{z}{b}\Big)^{1/2},$$

so that

$$\pi(x;b,a) - \pi(x-z;b,a) \ll \frac{z}{\phi(b)\log(z/b)},$$

which is what we wanted to prove. If on the other hand $z/b \le c_0$, then $[x, x-z]$ contains at most $z/b+1 \le c_0+1$ numbers congruent to $a \pmod b$, implying that the desired inequality is true with some appropriate implied constant anyway. This completes the proof of the theorem. □

12.7. Twin primes revisited

Again let $\mathcal{J}(x) = \#\{p \le x \ : \ p,\ p+2 \text{ are both primes}\}$. Brun's combinatorial sieve gives the following result.

Theorem 12.8. *The estimate*

$$\mathcal{J}(x) \ll \frac{x}{(\log x)^2}$$

holds.

Proof. We only sketch the proof. Again we choose $\mathcal{A} = \{n(n+2) \ : \ n \le x\}$, we let $y \le x$ be a number which will be chosen later and we set $\mathcal{P} = \{p \le y\}$. From the proof of Proposition 12.4, we know that

$$\mathcal{A}_d = x\frac{w(d)}{d} + R_d,$$

where $w(d)$ is the multiplicative function with $w(2) = 1$ and $w(p) = 2$ if p is an odd prime and $|R(d)| \le 2^{\omega(d)}$. It is easy to check that (ii) holds with $\kappa = 2$. We then apply the Brun combinatorial sieve. Note that the error term is $O(y^{2u})$, because $|R_d| \le 2^{\omega(d)} \ll d$ for all $d \le y^u$. Thus, we may choose $y = x^{1/4u}$, where $u > 0$ is an absolute constant and the error term is $O(x^{1/2})$. Hence, we get that

$$\mathcal{J}(x) \ll x\prod_{p\le y}\left(1 - \frac{2}{p}\right) + x^{1/2},$$

and the calculation used in the proof of Proposition 12.4 shows that

$$\prod_{p\le y}\left(1-\frac{2}{p}\right) \ll \frac{1}{(\log y)^2} = \frac{1}{(\log(x^{1/4u}))^2} \ll \frac{1}{(\log x)^2},$$

which completes the proof of the theorem. □

12.8. Smooth shifted primes

In this section, we prove the following result.

Theorem 12.9. *There exists a positive number $\rho < 1$ such that*

$$\#\{p \le x : P(p-1) < x^\rho\} \gg \frac{x}{\log x}.$$

Proof. Let $\rho = 1-\varepsilon$, where $\varepsilon > 0$ is fixed and assume that $P(p-1) > x^\rho$. Then $p-1 = aq$, where q is a prime and $a < x^\varepsilon$. Fix a. Then $q < x/a$ is a prime such that $aq+1$ is also a prime. We use the Brun sieve to estimate the number of such primes q. Take $\mathcal{A}_a = \{n(an+1) \ : \ n \le x/a\}$ and $\mathcal{P} = \{p \le y\}$, where y will be suitably chosen. It is easy to show (and we already did it several times by now) that if we write $w(d)$ for the number of solutions of $n(an+1) \equiv 0 \pmod d$ in $\{0,1,\dots,d-1\}$, then $w(d)$ is a multiplicative function (see, for example, Problem 12.4). When d is a prime, we have that $w(p) = 2$ if $p \nmid a$ and $w(p) = 1$ otherwise. Thus, condition (i) of Theorem 12.6 is satisfied with $|R_d| \le 2^{\omega(d)}$. One easily checks that condition (ii) is also satisfied with $\kappa = 2$ uniformly in a. Thus, one may apply Theorem 12.6 and get that, choosing $y < (x^{1/2})^{1/2u} < (x/a)^{1/2u}$ if $\varepsilon < 1/2$,

$$\begin{aligned}
\mathcal{S}(\mathcal{A}_a,\mathcal{P},y) &\ll \frac{x}{a}\prod_{2\le p\le y}\left(1-\frac{w(p)}{p}\right)\\
&\ll \frac{x}{a}\left(\frac{a}{\phi(a)}\right)\prod_{2\le p\le y}\left(1-\frac{1}{p}\right)^2\\
&\ll \frac{x}{\phi(a)}\frac{1}{(\log(x/a))^2}.
\end{aligned}$$

Since $a < x^{1/2}$, or $x/a > x^{1/2}$, it follows that

$$\mathcal{S}(\mathcal{A}_a,\mathcal{P},y) \ll \frac{x}{\phi(a)}\frac{1}{(\log x)^2}.$$

Summing up over all $a \le x^\varepsilon$, we get

$$\#\{p \le x \ : \ P(p-1) > x^{1-\varepsilon}\} \le \sum_{a\le x^\varepsilon}\mathcal{S}(\mathcal{A}_a,\mathcal{P},y) \ll \frac{x}{(\log x)^2}\sum_{a\le x^\varepsilon}\frac{1}{\phi(a)}.$$

Using the estimate (see Problem 12.9)

$$\sum_{a\le t}\frac{1}{\phi(a)} \ll \log t, \tag{12.14}$$

which is valid for all $t \ge 2$, we get that

$$\#\{p \le x \ : \ P(p-1) > x^{1-\varepsilon}\} \ll \frac{x\log(x^{\varepsilon})}{(\log x)^2} \ll \frac{\varepsilon x}{\log x}.$$

Hence, let c be the constant implied above. Then there are at most $c\varepsilon x/\log x$ primes $p \le x$ such that $P(p-1) > x^{1-\varepsilon}$. Choosing $\varepsilon = 1/2c$, we get that there are $\pi(x) - x/(2\log x) \ge x/(3\log x)$ primes $p \le x$ (for $x > x_0$) such that $P(p-1) < x^{1-1/2c}$, which is what we wanted to prove, with $\rho = 1 - 1/2c$.

□

The result proved in Theorem 12.9 has a rich history. Under the present form it was proved by Erdős [**47**] in 1935. He was 25 years old. Subsequently, many mathematicians obtained specific values of ρ for which Theorem 12.9 holds. These include C. Pomerance ($\rho = 0.48$), J. Friedlander [**61**] ($\rho = 1/2\sqrt{e} \approx 0.303$), and others. The current record-holders are Baker and Harman [**4**] with $\rho = 0.2936$. It is believed that Theorem 12.9 holds with any $\rho > 0$. In the opposite direction, Fouvry [**60**] showed that

$$\#\{p \le x \ : \ P(p-1) \ge x^{2/3}\} \gg \frac{x}{\log x}.$$

It is believed that the above estimate holds with $2/3$ replaced by $1-\varepsilon$ for any fixed $\varepsilon > 0$.

12.9. The Goldbach conjecture

Goldbach conjectured that every even positive integer ≥ 4 is a sum of two primes. This problem is called the *Goldbach conjecture* and at times the *Goldbach problem*. Let n be an even positive integer and write

$$T(n) = \#\{p \le n \ : \ n-p \text{ is prime}\}. \tag{12.15}$$

While we cannot prove that $T(n) > 0$ for all each integer $n > 2$, we can, however, obtain an upper bound for $T(n)$.

Theorem 12.10. *The inequality*

$$T(n) \ll \frac{n}{(\log n)^2}\prod_{p\,|\,n}\left(1+\frac{1}{p}\right)$$

holds.

Proof. We apply the Brun combinatorial sieve to the set $\mathcal{A} = \{m(n-m) \ : \ m \le n\}$. Let $X = n$. It is easy to check that one can take $w(p) = 2$ if $p \nmid n$ and $w(p) = 1$ if $p \mid n$. Hence, by the Brun sieve, one gets

$$T(n) \ll n \left(\frac{n}{\phi(n)}\right) \frac{1}{(\log n)^2},$$

and noticing that

$$\frac{n}{\phi(n)} = \frac{\gamma(n)}{\phi(\gamma(n))} \ll \frac{\sigma(\gamma(n))}{\gamma(n)} = \prod_{p \mid n} \left(1 + \frac{1}{p}\right),$$

the proof of the theorem is complete. □

It is conjectured that there exists a positive constant C_2 such that

$$\begin{aligned} T(N) &= \#\{p, q \ : \ p + q = N\} = 2C_2(1 + o(1)) \left(\prod_{\substack{p \mid N \\ p > 2}} \frac{p-1}{p-2}\right) \int_2^N \frac{dt}{(\log t)^2} \\ &= 2C_2(1 + o(1)) \frac{N}{(\log N)^2} \left(\prod_{\substack{p \mid N \\ p > 2}} \frac{p-1}{p-2}\right) \end{aligned}$$

as $N \to \infty$. It is known that this is true for all even $N \le x$ with a set of possible exceptions (called the exceptional Goldbach set) of cardinality $O(x^\delta)$ for some constant $\delta > 0$. Recent work of Li [**97**] shows that $\delta = 0.921$ is acceptable. As far as statements which are valid for all integers go, Chen [**23**] proved that every sufficiently large even integer n can be written in the form $n = p + q$, where p is prime and $q \in P_2$ (recall that a positive integer m is a P_k if $\Omega(m) \le k$). In fact, Chen proved much more. Here is a widely applicable version of Chen's theorem.

Theorem 12.11. *(Chen Theorem) Given an arbitrary positive even integer a, there exists $x_0 = x_0(a)$ such that for each $x > x_0(a)$, the interval $[x/2, x]$ contains a number $\gg x/(\log x)^2$ of primes p such $(p+1)/2a$ is an integer which is either a prime or a product of two primes each exceeding $x^{1/10}$.*

In fact, Chen proved it for $(p+1)/(2a)$ replaced by $N - p$, where $N = x$ is an even integer.

12.10. The Schnirelman theorem

Definition 12.12. *Let $\mathcal{A} = \{a_1, a_2, \ldots\}$ be a set of nonnegative integers and let $\mathcal{A}(x) = \#(\mathcal{A} \cap [1, x])$. Then*

$$\sigma(\mathcal{A}) = \inf_{n \geq 1} \frac{\mathcal{A}(n)}{n}$$

is called the Schnirelman density of $\mathcal{A}$.

If $\mathcal{A}$ and $\mathcal{B}$ are subsets of the set of real numbers, we let $\mathcal{A} + \mathcal{B} = \{a + b \ : \ a \in \mathcal{A}, \ b \in \mathcal{B}\}$.

Lemma 12.13. *If $\mathcal{A}$ and $\mathcal{B}$ are sets of nonnegative integers with $1 \in \mathcal{A}$ and $0 \in \mathcal{B}$, then*

$$\sigma(\mathcal{A} + \mathcal{B}) \geq \sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\sigma(\mathcal{B}).$$

Proof. Our proof is the one attributed to Schnirelman and appearing in Nathanson's book [**111**] (Theorem 7.5, page 193).

Let n be a fixed positive integer, let $a_1 < a_2 < \cdots$ be all the elements of $\mathcal{A}$, and assume that $\mathcal{A}(n) = r$. Divide $[1, n]$ into intervals $[a_i, a_{i+1})$ for $i = 1, \ldots, r-1$ and $[a_r, n]$. All numbers of the form $a_i + t$ with $1 \leq t \leq a_{i+1} - a_i - 1$ are in $\mathcal{A} \cap [a_i, a_{i+1})$ together with the numbers a_i since $0 \in \mathcal{B}$. Thus,

$$\begin{aligned}
(\mathcal{A} + \mathcal{B})(n) &\geq \sum_{i=1}^{r-1} (\mathcal{B}(a_{i+1} - a_i - 1) + 1) + \mathcal{B}(n - a_r) + 1 \\
&\geq r + \left(\sum_{i=1}^{r-1} (a_{i+1} - a_i - 1) + n - a_r \right) \sigma(\mathcal{B}) \\
&= r + (n - r)\sigma(\mathcal{B}) = \mathcal{A}(n)(1 - \sigma(\mathcal{B})) + n\sigma(\mathcal{B}) \\
&\geq n(\sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\sigma(\mathcal{B})),
\end{aligned}$$

which implies the desired inequality. □

Lemma 12.14. *Let $\mathcal{A}$ and $\mathcal{B}$ be sets of nonnegative integers such that $0 \in \mathcal{A} \cap \mathcal{B}$ and $\sigma(\mathcal{A}) + \sigma(\mathcal{B}) \geq 1$. Then $\sigma(\mathcal{A} + \mathcal{B}) = 1$, that is, $\mathcal{A} + \mathcal{B}$ is the set of all nonnegative integers.*

Proof. If $1 \notin \mathcal{A}$ then $\sigma(\mathcal{A}) = 0$, so that $\sigma(\mathcal{B}) = 1$ and we are done. Thus, assume that $1 \in \mathcal{A}$. Assume that there exists a natural number $n \notin \mathcal{A} + \mathcal{B}$. Since $0 \in \mathcal{B}$, we get that $n \notin \mathcal{A}$. But then

$$\mathcal{A}(n-1) = \mathcal{A}(n) \geq n\sigma(\mathcal{A}) > (n-1)\sigma(\mathcal{A})$$

and

$$\mathcal{B}(n-1) \geq (n-1)\sigma(\mathcal{B}),$$

so that

$$\mathcal{A}(n-1)+\mathcal{B}(n-1) > (n-1)(\sigma(\mathcal{A})+\sigma(\mathcal{B})) \geq n-1,$$

giving

$$\mathcal{A}(n-1)+\mathcal{B}(n-1) \geq n.$$

Let $a_1 < \cdots < a_r$ and $b_1 < \cdots < b_s$ be all the members of $\mathcal{A}$ and of $\mathcal{B}$ that are $\leq n-1$, respectively. Then the $r+s$ integers $a_1, \ldots, a_r, n-b_1, \ldots, n-b_s$ are all positive and $< n$. Since there are $r+s \geq n$ of these numbers, by the Pigeon Hole principle, two of them must coincide, so that there must exist i and j such that $a_i = n-b_j$. Thus, $n = a_i + b_j \in \mathcal{A}+\mathcal{B}$, which is the desired contradiction. □

Definition 12.15. *A set $\mathcal{A}$ consisting of some positive integers and 0 is called a base of order c if*

$$\underbrace{\mathcal{A}+\cdots+\mathcal{A}}_{c \text{ times}}$$

consists of all the nonnegative integers. That is, every positive integer is a sum of at most c terms from $\mathcal{A}$.

Lemma 12.16. *If $\sigma(\mathcal{A}) > 0$, then $\mathcal{A}$ is a base of finite order.*

Proof. Let $\mathcal{A}_2 = \mathcal{A}+\mathcal{A}$ and define recursively $\mathcal{A}_r = \mathcal{A}+\mathcal{A}_{r-1}$ for all $r \geq 3$. Let $\alpha = \sigma(\mathcal{A})$. By Lemma 12.13,

$$\sigma(\mathcal{A}_2) \geq 2\alpha - \alpha^2 = 1-(1-\alpha)^2.$$

By induction, one can show that, for all integers $r \geq 2$,

$$\sigma(\mathcal{A}_r) \geq 1-(1-\alpha)^r,$$

where the induction step is based on Lemma 12.13 with $\mathcal{B} = \mathcal{A}_r$. Since $\alpha > 0$, there exists r such that $(1-\alpha)^r < 1/2$. Then $\sigma(\mathcal{A}_r) > 1/2$, so that Lemma 12.14 shows that $\mathcal{A}_{2r} = \mathcal{A}_r + \mathcal{A}_r$ contains all the nonnegative integers. □

We can now prove Schnirelman's theorem.

Theorem 12.17. *(Schnirelman) There exists a constant $c > 0$ such that every integer $n \geq 2$ is a sum of at most c primes.*

Proof. We start by showing that the set $\mathcal{Q}$ consisting of 0, 1 and the numbers which are a sum of two primes has a positive Schnirelman density. Let

$$\mathcal{Q}(x) = \{m \leq x \ : \ m \in \mathcal{Q}\}.$$

By the Cauchy-Schwarz inequality (see (1.20)), we get that, with $T(n)$ defined in (12.15),

(12.16)
$$\left(\sum_{n\le x} T(n)\right)^2 \le \left(\sum_{n\le x} T^2(n)\right)\left(\sum_{m\in\mathcal{Q}(x)} 1\right) \le \left(\sum_{n\le x} T^2(n)\right) \times \#\mathcal{Q}(x).$$

Note that for $x \ge 4$,

$$\sum_{n\le x} T(n) \ge \sum_{p_1,p_2\le x/2} 1 = \pi(x/2)^2 \gg \frac{x^2}{(\log x)^2}, \tag{12.17}$$

while by Theorem 12.10 and the inequality

$$[d_1,d_2]^2 \ge [d_1,d_2](d_1,d_2) = d_1d_2,$$

which implies that $[d_1,d_2] \ge (d_1d_2)^{1/2}$, we have

$$\begin{aligned}\sum_{n\le x} T^2(n) &\ll \frac{x^2}{(\log x)^4}\sum_{n\le x}\prod_{p\mid n}\left(1+\frac{1}{p}\right)^2\\ &\ll \frac{x^2}{(\log x)^4}\sum_{n\le x}\left(\sum_{d\,\mid\, n}\frac{1}{d}\right)^2\\ &= \frac{x^2}{(\log x)^4}\sum_{n\le x}\left(\frac{\sigma(n)}{n}\right)^2\\ &\ll \frac{x^3}{(\log x)^4},\end{aligned} \tag{12.18}$$

where we used the second estimate of Problem 8.10.

Inserting both the lower bound (12.17) and the upper bound (12.18) into inequality (12.16), we get

$$\frac{x^4}{(\log x)^4} \ll \#\mathcal{Q}(x)\frac{x^3}{(\log x)^4},$$

giving $\#\mathcal{Q}(x) \gg x$. Now Lemma 12.16 tells us that there exists a constant c such any positive integer n is of the form $a_1+\cdots+a_i$ for some $i \le c' \le c$, where $a_i = 1$ or a_i is a prime. Now let $m \ge 2$ be an integer. Applying what we concluded above for $m-2$, we get

$$m-2 = \sum_{i\le k} 1 + \sum_{k<i\le c'} p_i,$$

where the p_i's are some primes. If $k = 0$ or $k = 1$, then

$$m = p + \sum_{k<i\le c'} p_i,$$

where $p = 2,\ 3$, while if $k \ge 2$, we then write

$$k = \underbrace{2 + \cdots + 2}_{\kappa \text{ times}} + \underbrace{3 + \cdots + 3}_{\ell \text{ times}}$$

for some nonnegative integers $\kappa,\ \ell$ with $\kappa + \ell < k$, and we still get that

$$m = \underbrace{2 + \cdots + 2}_{\kappa+1 \text{ times}} + \underbrace{3 + \cdots + 3}_{\ell \text{ times}} + \sum_{k<i\le c'} p_i$$

is a sum of at most $c' \le c$ primes, which is what we wanted to prove. □

Schnirelman showed that $c = 300\,000$ is acceptable in Theorem 12.17. While the Goldbach problem is out of reach, Vinogradov proved in 1937 the following remarkable theorem.

Theorem 12.18. *Let $r(N)$ be the number of prime triplets (p, q, r) such that $N = p + q + r$. Then, as $N \to \infty$,*

$$r(N) = \frac{C_3}{2}(1 + o(1))\frac{N^2}{(\log N)^3} \prod_{p \mid N} \left(1 - \frac{1}{p^2 - 3p + 3}\right),$$

where

$$C_3 = \prod_{p \ge 2} \left(1 + \frac{1}{(p-1)^3}\right).$$

Hence, in particular, every large odd positive integer is a sum of three primes.

As we mentioned before, it is not known that both p and $p+2$ are primes infinitely often. It is also not known that $n^2 + 1$ is prime infinitely often. Each prime $p \equiv 1 \pmod 4$ is a sum of two squares, so that $a^2 + b^2$ is a prime infinitely often. A few years ago, J. Friedlander and H. Iwaniec [**62**] obtained the following fascinating result:

Theorem 12.19. *There exists a constant $\kappa > 0$ such that*

$$\#\{n \le x \ :\ n = a^2 + b^4 \text{ for some integers } a \text{ and } b\} = \kappa(1 + o(1))\frac{x^{3/4}}{\log x}$$

as $x \to \infty$.

In particular, the polynomial $X^2 + Y^4$ represents infinitely many primes. The method of Friedlander and Iwaniec was suitably adapted by Heath-Brown [**79**] to yield infinitely many primes of the form $X^3 + 2Y^3$. Before this, it was unknown if there were infinitely many primes of the form $a^3 + b^3 + c^3$ with positive integers a, b and c. These theorems are among the highest achievements nowadays in sieve methods. We will not prove any of them, but rather discuss another elementary sieve, namely Selberg's sieve.

12.11. The Selberg sieve

The Selberg sieve is an upper bound sieve which is remarkable by the simplicity of its basic idea. Assume, for simplicity, that $\mathcal{A} = \{h(n) : n \le x\}$ where $h(X) \in \mathbb{Z}[X]$ is a nonconstant polynomial. Let $w(d) = \#\{0 \le n \le d-1 \ : \ h(n) \equiv 0 \pmod d\}$, let $\mathcal{P}$ be a set of primes and put $P(y) = \prod_{\substack{p \le y \\ p \in \mathcal{P}}} p$. Assume that $1 \le w(p) < p$ for all $p \mid P(y)$. Let

$$\mathcal{A}_d = x\frac{w(d)}{d} + R(d),$$

where $|R_d| \le w(d)$. Recall that in order to get an upper bound on $\mathcal{S}(\mathcal{A}, \mathcal{P}, y)$ we need to find some multiplicative function $\lambda(d)$, such that

$$\sum_{d|(n,P(y))} \mu(d) \le \sum_{d|(n,P(y))} \lambda(d) \tag{12.19}$$

and once the above inequality is true for all positive integers n, the arguments from Section 1 (the sieve of Eratosthenes) show that

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, y) \le x \sum_{d \,|\, P(y)} \frac{\lambda(d)w(d)}{d} + \sum_{d \,|\, P(y)} \lambda(d)R(d). \tag{12.20}$$

Selberg's idea was to let Φ be some multiplicative function and to define $\lambda(d)$ via

$$\sum_{d \,|\, (n,P(y))} \lambda(d) = \left(\sum_{d \,|\, (n,P(y))} \Phi(d) \right)^2, \tag{12.21}$$

in which case inequality (12.19) holds because its right-hand side is always ≥ 0 and it is 1 if $(n, P(y)) = 1$ because $\Phi(1) = 1$. This suggests defining

$$\lambda(d) = \sum_{\substack{d_1, d_2 | P(y) \\ d = [d_1, d_2]}} \Phi(d_1)\Phi(d_2)$$

and $\lambda(p) = 0$ if $p \nmid P(y)$, in which case identity (12.21) is clearly satisfied. In order to optimize the result, Selberg went on to find Φ in such a way that the main term in (12.20) is optimal, that is, is as small as possible. Remarkably, the function Φ that optimizes this problem exists, is unique, and can be computed. For this, put $f(d) = d/w(d)$ for all $d \mid P(y)$ and let

$$g(k) = f(k) \prod_{p \,|\, k} \left(1 - \frac{w(p)}{p}\right) \qquad (k \mid P(y)).$$

Note that $g(k) > 0$ for all $k \mid P(y)$, and since all k's under scrutiny are squarefree and f is multiplicative, we get that if $d \mid k$, then d and k/d are

coprime, so that $f(k) = f(d(k/d)) = f(d)f(k/d)$, and therefore

$$g(k) = f(k)\prod_{p\,|\,k}\left(1 - \frac{1}{f(p)}\right) = \sum_{d\,|\,k}\mu(d)\frac{f(k)}{f(d)} = \sum_{d\,|\,k}\mu(d)f\left(\frac{k}{d}\right).$$

Thus, $g = \mu * f$, that is,

$$f(k) = \sum_{d\,|\,k} g(d).$$

Note also that since $(d_1, d_2)[d_1, d_2] = d_1 d_2$, we have that

$$f([d_1, d_2]) = f\left(d_1\left(\frac{d_2}{(d_1, d_2)}\right)\right) = f(d_1)f\left(\frac{d_2}{(d_1, d_2)}\right) = \frac{f(d_1)f(d_2)}{f((d_1, d_2))},$$

so that

$$\frac{1}{f([d_1, d_2])} = \frac{1}{f(d_1)f(d_2)}f((d_1, d_2)) = \frac{1}{f(d_1)f(d_2)}\sum_{d|(d_1,d_2)} g(d).$$

Selberg then sets

$$Q = \sum_{d\,|\,P(y)}\frac{1}{g(d)} = \sum_{d\,|\,P(y)}\frac{w(d)}{d}\prod_{p\,|\,d}\left(1 - \frac{w(p)}{p}\right)^{-1},$$

and proves the following theorem.

Theorem 12.20. *Let Φ be a multiplicative function with $\Phi(p) = 0$ if $p \nmid P(y)$. Set*

$$\lambda(d) = \sum_{\substack{d_1, d_2 | P(y)\\ [d_1,d_2]=d}} \Phi(d_1)\Phi(d_2)$$

and let $\lambda(d) = 0$ if $d \nmid P(y)$. Then

$$\sum_{d\,|\,P(y)}\frac{\lambda(d)}{f(d)} \geq \frac{1}{Q}, \tag{12.22}$$

with equality if and only if

$$\Phi(d) = \frac{1}{Q}\mu(d)f(d)\sum_{t|d}\frac{1}{g(t)} \qquad (d \mid P(y)).$$

Proof. Let $H(\Phi)$ be the expression appearing on the left-hand side of inequality (12.22). Then

$$\begin{aligned} H(\Phi) &= \sum_{d_1,d_2|P(y)}\frac{\Phi(d_1)\Phi(d_2)}{f([d_1, d_2])} = \sum_{d_1,d_2|P(y)}\frac{\Phi(d_1)}{f(d_1)}\frac{\Phi(d_2)}{f(d_2)}\sum_{t|(d_1,d_2)} g(t)\\ &= \sum_{t\,|\,P(y)} g(t)\sum_{\substack{d_1\,|\,P(y),\ d_2\,|\,P(y)\\ t\,|\,d_1,\ t\,|\,d_2}}\frac{\Phi(d_1)\Phi(d_2)}{f(d_1)f(d_2)} \end{aligned}$$

$$= \sum_{t \mid P(y)} g(t) \left(\sum_{\substack{d \mid P(y) \\ t \mid d}} \frac{\Phi(d)}{f(d)} \right)^2 .$$

Choose

$$y(t) = \sum_{\substack{d \mid P(y) \\ t \mid d}} \frac{\Phi(d)}{f(d)}$$

and observe that

$$\Phi(d) = f(d) \sum_{\substack{t \mid P(y) \\ d \mid t}} \mu\left(\frac{t}{d}\right) y(t). \tag{12.23}$$

Setting $d = 1$, we get $1 = \sum_{t \mid P(y)} \mu(t) y(t)$. Hence,

$$\begin{aligned} H(\Phi) &= \sum_{t \mid P(y)} g(t) y^2(t) \\ &= \sum_{t \mid P(y)} g(t) y^2(t) - \frac{2}{Q} \sum_{t \mid P(y)} \mu(t) y(t) + \frac{1}{Q^2} \sum_{t \mid P(y)} \frac{\mu^2(t)}{g(t)} + \frac{1}{Q} \qquad (12.24) \\ &= \sum_{t \mid P(y)} \frac{1}{g(t)} \left(g(t) y(t) - \frac{\mu(t)}{Q} \right)^2 + \frac{1}{Q}. \end{aligned}$$

Thus, $H(\Phi) \geq 1/Q$, which is what we wanted to prove. It remains to be seen when the minimum is achieved. In fact, it is clear from (12.24) that the minimum is obtained precisely when

$$y(t) = \frac{\mu(t)}{Q g(t)}.$$

Substituting this value in (12.23), we get

$$\Phi(d) = \frac{f(d)}{Q} \sum_{\substack{t \mid P(y) \\ d \mid t}} \frac{\mu(t)}{g(t)} \mu\left(\frac{t}{d}\right) = \frac{f(d)\mu(d)}{Q} \sum_{\substack{t \mid P(y) \\ d \mid t}} \frac{1}{g(t)}, \tag{12.25}$$

which is the other result we needed to prove. □

Using the above result, we get the following sieving result.

Theorem 12.21. *With the notations from the preceding theorem,*

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, y) \leq \frac{x}{Q} + y^2 \prod_{p \mid P(y)} \left(1 - \frac{w(p)}{p}\right)^{-2}.$$

Proof. The main term is easy to obtain. It remains to bound

$$R = \sum_{d_1,d_2|P(y)} |\Phi(d_1)\Phi(d_2)R([d_1,d_2])|.$$

But, in light of (12.25),

$$|\Phi(d)| = \frac{f(d)}{Q} \sum_{\substack{t|\,P(y)\\ d\,|\,t}} \frac{1}{g(t)} \le \frac{f(d)}{g(d)Q} \sum_{k\,|\,P(y)} \frac{1}{g(k)} \le \frac{f(d)}{g(d)}$$

and since

$$|R([d_1,d_2])| \le \frac{[d_1,d_2]}{f([d_1,d_2])} = \frac{d_1d_2}{(d_1,d_2)} \cdot \frac{f((d_1,d_2))}{f(d_1)f(d_2)} \le \frac{d_1}{f(d_1)} \frac{d_2}{f(d_2)},$$

we get that

$$\begin{aligned} R &\le \sum_{d_1,d_2\,|\,P(y)} \frac{f(d_1)}{g(d_1)} \frac{f(d_2)}{g(d_2)} \frac{d_1}{f(d_1)} \frac{d_2}{f(d_2)} \\ &\le \left(\sum_{d\,|\,P(y)} \frac{d}{g(d)} \right)^2 \le y^2Q^2, \end{aligned}$$

while it is clear that

$$Q \le \prod_{p\le y} \left(1 + \frac{1}{g(p)}\right).$$

Finally, since

$$1 + \frac{1}{g(p)} = 1 + \frac{1}{f(p)-1} = \left(1 - \frac{1}{f(p)}\right)^{-1} = \left(1 - \frac{w(p)}{p}\right)^{-1},$$

the desired estimate follows. □

12.12. The Brun-Titchmarsh theorem from the Selberg sieve

At this point, it is illuminating to explain how one can deduce the Brun-Titchmarsh theorem from the Selberg sieve. Let $h(n) = a + bn$, and assume that $bn + a \le x$. Then $n \le \lfloor x/b \rfloor + 1 \le 2x/b$ for $b < x$. Let y be a parameter to be fixed later. Note that $\mathcal{P} = \{p : p \nmid b\}$ and that $w(p) = 1$ for all $p \mid P(y)$. Thus, $f(d) = d$ and therefore

$$g(d) = d \prod_{p\,|\,d} \left(1 - \frac{1}{p}\right) = \phi(d).$$

Hence,

$$Q = \sum_{d \mid P(y)} \frac{1}{\phi(d)} = \sum_{\substack{d \le y \\ (d,b)=1}} \prod_{p \mid d} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \ge \sum_{\substack{d \le y \\ (d,b)=1}} \frac{1}{d}.$$

Since

$$\begin{aligned} \prod_{p \mid b} \left(1 - \frac{1}{p}\right)^{-1} \left(\sum_{\substack{d \le y \\ (d,b)=1}} \frac{1}{d}\right) &= \prod_{p \mid b} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) \left(\sum_{\substack{d \le y \\ (d,b)=1}} \frac{1}{d}\right) \\ &\ge \sum_{m \le y} \frac{1}{m} > \log y, \end{aligned}$$

we get that

$$Q > (\log y) \prod_{p \mid b} \left(1 - \frac{1}{p}\right) = \frac{\phi(b)}{b} \log y.$$

We also have that

$$y^2 \prod_{p \le y} \left(1 - \frac{1}{p}\right)^{-2} \ll y^2 (\log y)^2.$$

Thus,

$$\mathcal{S}(\mathcal{A}, \mathcal{P}, y) \ll \frac{x}{b} \left(\frac{b}{\phi(b)}\right) \frac{1}{\log y} + y^2 (\log y)^2 = \frac{x}{\phi(b) \log y} + y^2 (\log y)^2.$$

Choosing $y = (x/b)^{1/3}$, it follows that

$$\pi(x; b, a) \ll \frac{x}{\phi(b) \log(x/b)},$$

which is precisely the Brun-Titchmarsh theorem (Theorem 12.7).

12.13. The Large sieve

The Large sieve was invented in 1941 by Linnik and thereafter improved by Bombieri [**14**], Montgomery-Vaughan [**107**], and others. Here we state without proof its most modern version.

Let $\{a_n\}_{n=1,\dots,N}$ be a sequence of complex numbers and let

$$w(p) = \#\{h : 0 \le h \le p-1 \ \text{ and } \ n \equiv h \bmod p \Longrightarrow a_n = 0\},$$

and again assume that $w(p) < p$ for all primes p. Set

$$g(d) = \mu(d)^2 \prod_{p \mid d} \frac{w(p)}{p - w(p)}. \tag{12.26}$$

Then the Large sieve is the following result.

Theorem 12.22. *If* $L = \sum_{d \le Q} g(d)$, *then*

$$\left| \sum_{n=1}^{N} a_n \right|^2 \le \frac{N - 1 + Q^2}{L} \sum_{n=1}^{N} |a_n|^2. \tag{12.27}$$

12.14. Quasi-squares

We now give an application of the Large sieve. A positive integer n is called a *quasi-square* if the congruence $n \equiv x^2 \pmod{p}$ has an integer solution x for each prime number $p \le n^{1/2}$. Clearly, all squares are quasi-squares, but are there more quasi-squares than squares? The next result shows that the number of quasi-squares up to x is of the same order of magnitude as the number of squares up to x.

Proposition 12.23. *Let* $\mathcal{Q} = \{n : n \text{ is quasi-square}\}$. *Then* $\#(\mathcal{Q} \cap [1, x]) \ll x^{1/2}$.

Proof. Let $\mathcal{Q}_1(x)$ be the set of quasi-squares in $[x/2, x]$. Let $a_n = 1$ if $n \in \mathcal{Q}_1(x)$ and $a_n = 0$ otherwise. For each prime $p \le (x/2)^{1/2}$, there are precisely $(p-1)/2$ congruence classes $h \pmod{p}$ which are not quadratic residues modulo p. For such classes $h \pmod{p}$, the congruence $a \equiv h \pmod{p}$ is impossible for all $a \in \mathcal{Q}_1(x)$. Thus, we may take $w(p) = (p-1)/2$, $N = x$ and $Q = (x/2)^{1/2}$ in the Large sieve and get

$$(\#\mathcal{Q}_1(x))^2 = \left| \sum_{n \le x} a_n \right|^2 \le \frac{x - 1 + x/2}{L} \sum_{n \le x} |a_n|^2 < \frac{3x}{2L} \#\mathcal{Q}_1(x),$$

leading to $\#\mathcal{Q}_1(x) \ll x/L$. Note that $w(p)/(p - w(p)) = (p-1)/(p+1)$, so that if $\mu(d) \ne 0$, then $g(d)$ defined in (12.26) satisfies

$$\begin{aligned} g(d) &\gg \prod_{p \mid d} \left(\frac{p-1}{p+1} \right) = \prod_{p \mid d} \left(1 - \frac{2}{p+1} \right) \\ &= \prod_{p \mid d} \left(1 - \frac{1}{p} \right)^2 \prod_{p \mid d} \left(1 - \frac{2}{p+1} \right) \left(1 - \frac{1}{p} \right)^{-2} \\ &= \left(\frac{\phi(d)}{d} \right)^2 \prod_{p \mid d} \left(1 - \frac{1}{p^2} \right)^{-1}. \end{aligned} \tag{12.28}$$

Since the product

$$\prod_p \left(1 - \frac{1}{p^2}\right)^{-1}$$

converges (to $\zeta(2)$), it follows from formula (12.28) that $g(d) \gg (\phi(d)/d)^2$. Thus,

$$L = \sum_{d \le Q} g(d) \gg \sum_{d \le Q} \left(\frac{\phi(d)}{d}\right)^2 \gg Q,$$

where we used the first estimate of Problem 8.10.

Thus,

$$\mathcal{Q}_1(x) \ll \frac{x}{Q} \ll x^{1/2}.$$

Changing x to $x/2$, then to $x/4$, and so on, we then get that the total number of quasi-squares $n \le x$ is

$$\begin{aligned} \#(\mathcal{Q} \cap [1,x]) &\ll \sum_{0 \le k \le \log x/\log 2} \#\mathcal{Q}_1(x/2^k) \\ &\ll \sum_{0 \le k \le \log x/\log 2} \left(\frac{x}{2^k}\right)^{1/2} \le x^{1/2} \sum_{k \ge 0} \frac{1}{2^{k/2}} \ll x^{1/2}, \end{aligned}$$

which completes the proof of the proposition. □

Remark 12.24. *The Large sieve is very useful because it is very general. It allows us to sieve off large chunks of the residue classes modulo p, as in the problem of the quasi-squares where we sieved off half of the residue classes modulo p for all primes p up to almost $x^{1/2}$. It is also very useful in conjunction with classical estimates like the Chebyshev estimates, the Brun-Titchmarsh estimates and the counting function of the twin primes where it gives small values for the implied constants. We shall not enter into the details or discuss the Large sieve inequalities that have been designed.*

12.15. The smallest quadratic nonresidue modulo p

Given an integer a and an odd prime p, we define the *Legendre symbol* of a with respect to p as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } p \nmid a \text{ and } x^2 \equiv a \pmod{p} \text{ for some integer } x, \\ -1 & \text{otherwise.} \end{cases} \tag{12.29}$$

We now give the following application (due to Linnik) that allows us to estimate the least quadratic nonresidue modulo p, that is, the smallest

positive integer $q(p)$ such that $\left(\frac{q(p)}{p}\right) = -1$. Notice that $q(p)$ is prime. It is conjectured that

$$q(p) \ll p^{\varepsilon} \tag{12.30}$$

for any $\varepsilon > 0$ with the implied constant depending on ε, but the best-known estimate is that the inequality (12.30) holds only for $\varepsilon > 1/(4\sqrt{e}) \approx 0.1516$.

Theorem 12.25. *The number of primes $p \le x$ such that $q(p) > x^{\varepsilon}$ is bounded by a constant depending on ε.*

Proof. Let

$$\mathcal{P} = \{p \le x^{1/2} : (n/p) = 1 \text{ for all } n \le x^{\varepsilon}\}$$

and observe that it is enough to show that $\#\mathcal{P} = O_{\varepsilon}(1)$, since afterwards the conclusion will follow by replacing ε with $\varepsilon/2$ and x by x^2. For every prime p, let

$$\Omega_p = \{\nu \pmod p) : (\nu/p) = -1\},$$

and let $\{a_n\}_{n \le x}$ be the characteristic function of the set

$$X = \{1 \le n \le x : (n/p) = 1 \text{ for all } p \in \mathcal{P}\}.$$

Then inequality (12.27) with $N = \lfloor x \rfloor$ and $Q = \sqrt{x}$ implies that

$$L \le \frac{N - 1 + Q^2}{\#X} < \frac{2x}{\#X}. \tag{12.31}$$

Observe that if $d = p \in \mathcal{P}$ is odd, then $w(p) = \#\Omega_p = (p-1)/2$, so that

$$g(p) = \frac{(p-1)/2}{p - (p-1)/2} = \frac{p-1}{p+1} \ge \frac{1}{2} \qquad \text{for all} \quad p \in \mathcal{P}.$$

Hence, inequality (12.31) yields

$$\#\mathcal{P} \le 2 \sum_{p \in \mathcal{P}} g(p) \le 2L \le \frac{4x}{\#X},$$

meaning that it suffices to prove that $\#X \gg_{\varepsilon} x$. Since X contains the set $\{n \le x : P(n) \le x^{\varepsilon}\}$, we can write that

$$\#X \ge \Psi(x, x^{\varepsilon}) \ge \frac{1}{2}\rho(1/\varepsilon)x \qquad \text{for} \quad x > x_{\varepsilon},$$

where the last inequality follows from Theorem 9.3, thus completing the proof of the theorem. □

Problems on Chapter 12

Problem 12.1. *Let x be large and set $y = \log x$.*

(i) *By observing that the number of positive integers $n \le x$ divisible by p^2 is $\le x/p^2$, show that the set of positive integers $n \le x$ which are multiples of p^2 for some prime $p > y$ is $O(x/y)$.*

(ii) *Use the Inclusion-Exclusion principle to show that the number of $n \le x$ which are not divisible by p^2 for any prime $p \le y$ is*

$$x \prod_{p \le y} \left(1 - \frac{1}{p^2}\right) + O(2^y).$$

(iii) *Let $\mathcal{S}(x) = \{n \le x : \mu(n) \neq 0\}$. Deduce from (i) and (ii) that*

$$\#\mathcal{S}(x) = \frac{6x}{\pi^2} + O\left(\frac{x}{\log x}\right).$$

Problem 12.2. *Let $A = \{n = |u^w \pm v!| \text{ for some integers } u,\ v,\ w > 1\}$. Let x be a large positive real number.*

(i) *Put $y = \log x/(\log\log x)^2$. Show that if x is large, then the set of $n \in A \cap [1, x]$ such that $v \le y$ is of cardinality $x^{1/2+o(1)}$ as $x \to \infty$.*

(ii) *From now on, assume that $v > y$. By noting that if $m > 2p$, then $p^2 \mid m!$, prove that if $n = |u^w \pm v!|$ with $w > 1$ and $p < y/2$, then either p is coprime to n or $p^2 \mid n$.*

(iii) *Let $z = \log\log x$. Show that the number of positive integers $n \le x$ divisible by p^2 for some $p > z$ is $O(x/\log\log x)$.*

(iv) *Show that if $n \in A \cap [1, x]$ is not as in (i) or (iii), then n is coprime with all the primes in $[z, y/2]$. Then use the Eratosthenes sieve to show that the number of such $n \le x$ is $O(x \log\log\log x/\log\log x) = o(x)$ as $x \to \infty$.*

(v) *Deduce that A is of asymptotic density zero.*

Problem 12.3. *Here is a more general version of the Eratosthenes sieve. Let $m_1, \dots, m_k$ be coprime positive integers. For each $i \in \{1, \dots, k\}$, let $\mathcal{A}_j = \{a_{i_1} \pmod{m_j}, \dots, a_{i_{\omega_j}} \pmod{m_j}\} \subset \mathbb{Z}/m_j\mathbb{Z}$ be a set of $\omega_j < m_j$ congruence classes modulo m_j. Put $\Omega = \max\{\omega_j : j = 1, \dots, k\}$. Let*

$$\mathcal{N} = \{n \le x : n \notin \mathcal{A}_j \pmod{m_j} \text{ for all } j = 1, \dots, k\}.$$

Show, using the Chinese Remainder Theorem and the Inclusion-Exclusion principle, that

$$\#\mathcal{N} = x \prod_{j=1}^{k} \left(1 - \frac{\omega_j}{m_j}\right) + O((\Omega + 1)^k).$$

Problem 12.4. *Let $f(X) \in \mathbb{Z}[X]$ be a nonconstant polynomial of degree D without double roots. Let*

$$\rho(d) = \#\{0 \le n \le d-1 \ : \ f(n) \equiv 0 \pmod{d}\}.$$

(i) *Show that ρ is a multiplicative function.*

Now, assume that

$$f(X) = \prod_{i=1}^{D}(a_i X + b_i),$$

where $a_i > 0$ and b_i are integers for $i = 1, \dots, D$.

(ii) *Show that the condition that $f(X)$ does not have double roots is equivalent to*

$$\Delta(f) = \prod_{i=1}^{D} \prod_{1 \le i < j \le D} (a_i b_j - a_j b_i) \neq 0.$$

(iii) *Show that $\rho(p) = D$ is equivalent to $gcd(p, \Delta(f)) = 1$.*

Problem 12.5. *Adapt the proof of Theorem 12.3 to show that if $f(X) \in \mathbb{Z}[X]$ is of degree D and such that $\rho(p) < p$ for every prime number p, then the set $\mathcal{A}_f = \{n \le x \ : \ p(f(n)) > y\}$ has cardinality*

$$x \prod_{p \le y} \left(1 - \frac{\rho(p)}{p}\right)\left(1 + O\left(\frac{1}{\log y}\right)\right),$$

provided that $x > x_D$ and $y \le \exp(\log x/(10D \log\log x))$.

Problem 12.6. *Let $L_i(X) = a_i X + b_i$, $i = 1, \dots, k$, be distinct linear forms with integer coefficients. Assume that $\gcd(a_i, b_i) = 1$ for $i = 1, \dots, k$, and that $a_i > 0$ for all $i = 1, \dots, k$. Moreover, for each prime p, let*

$$\nu(p) = \#\{0 \le n \le p-1 : a_i n + b_i \equiv 0 \pmod{p} \ \text{ for some } i = 0, 1, \dots, k\}.$$

(i) *Show that if we choose $f(X) = \prod_{i=1}^{k} L_i(X)$, then $\nu(p)$ coincides with $\rho(p)$ defined in Problem 12.4.*

(ii) *Use Problem 12.5 to show that*

$$\begin{aligned} &\#\{n \le x : a_i n + b_i \text{ is prime for all } i = 1, \dots, k\} \\ &\quad \le c(k)\left(\frac{\Delta(f)}{\phi(\Delta(f))}\right)^k \frac{x(\log\log x)^k}{(\log x)^k}, \end{aligned}$$

for $x > x(k)$ (some initial value depending only on k), where $c(k)$ is a constant that depends only on k. (Hint: Use Problem 12.5 with

$y = \exp(\log x/(10k \log\log x))$. *As for the main term, note that, by Problem* 12.4, *it is*

$$\leq \prod_{\substack{p\leq y \\ p>k,\ p\nmid\Delta(f)}} \left(1-\frac{k}{p}\right).$$

Prove first that if we put $a_k(p) = (1-k/p)/(1-1/p)^k$, *then* $\prod_{p>k} a_k(p)$ *converges to a positive number, so that the above product is bounded by*

$$c_1(k) \prod_{\substack{p\leq y \\ p>k,\ p\nmid\Delta(f)}} \left(1-\frac{1}{p}\right)^k,$$

where $c_1(k)$ *depends only on* k. *Finally observe that this last product runs over all the primes* p *with* $k < p \leq y$, *a contribution depending only on* k, *and the possible primes dividing* $\Delta(f)$. *What does the product of these eliminated factors have to do with* $\Delta(f)/\phi(\Delta(f))$? *Use also known results about the full product* $\prod_{p\leq y}(1-1/p)^k$.)

Problem 12.7. *Let* $\mathcal{A}$ *be the set of all positive integers* n *such* $d + n/d$ *is a prime for all divisors* d *of* n. *For example,* $n = 10$ *has this property because* $d + n/d \in \{1+10, 2+5\} = \{11, 7\}$. *Show that the sum of the reciprocals of the members of* $\mathcal{A}$ *is convergent. (Hint: Note that if* $n > 2$ *then* $n+1 = p$ *is prime, implying that* n *is even. Thus,* $2 + n/2 = q$ *is also prime. What is the relation between* p *and* q?)

Problem 12.8. *The following problem appeared as a conjecture in a recent paper of Elliott and Richner* [**44**]: *Show that the set* $\mathcal{A} = \{n \ : \ n = p^2 - q^2$ *with primes* $p,\ q\}$ *is of asymptotic density zero. Prove this result in the following way:*

(i) *Show that if* $n \in \mathcal{A}$, *then* $n = uv$, *where* $v < u$ *are positive integers, and that there exists a prime* q *such that* $p = q + v$ *is prime and* $u = p + q = 2q + v$. *Deduce that* $n \leq x$ *is determined by a positive integer* $v \leq x^{1/2}$ *and a prime* $q < x/v$ *such that* $p = q + v$ *is also a prime.*

(ii) *Use Problem* 12.6, *or adapt the proof of Proposition* 12.4, *to deduce that the number of primes* $q \leq x/v$ *such that* $q + v$ *is also a prime is*

$$\ll \left(\frac{v}{\phi(v)}\right) \frac{x}{v} \frac{(\log\log(x/v))^2}{(\log(x/v))^2}.$$

(iii) *Show that the above upper bound is*

$$\ll \frac{x(\log\log x)^3}{v(\log x)^2}.$$

(Hint: Use the maximal order of the function $m/\phi(m)$ in the interval $[1,x]$ and remember that $v \le x^{1/2}$.)

(iv) *Now sum up over $v \le x^{1/2}$ and conclude.*

Problem 12.9. *Prove the estimate* $\displaystyle\sum_{n\le t}\frac{1}{\phi(n)} \ll \log t$ *in the following way:*

(i) *First recall that $n/\phi(n) \ll \sigma(n)/n$ and deduce that*

$$\sum_{n\le x}\frac{1}{\phi(n)} \ll \sum_{n\le x}\frac{\sigma(n)}{n^2}.$$

(ii) *To compute the sum appearing on the right-hand side of the above estimate, use the known average value of $\sigma(n)/n$ in the interval $[1,x]$ (Problem 7.2) with the Abel summation formula for $a_n = \sigma(n)/n$ and $f(t) = 1/t$ to conclude that the sum appearing on the right-hand side of the above estimate is $\ll \log x$.*

Problem 12.10. *Use the Brun-Titchmarsh theorem and Abel's summation formula to show that*

$$\sum_{\substack{p\le x\\ p\equiv a \pmod b}}\frac{1}{p} \ll \frac{1}{p_{a,b}} + O\left(\frac{\log\log x}{\phi(b)}\right)$$

uniformly for $x \ge e^e$ and $1 \le a < b$, where a and b are coprime and $p_{a,b}$ is the smallest prime congruent to a modulo b, and where the constant implied by the above O is absolute.

The purpose of the following two problems is to learn something interesting about the distance between consecutive primes.

Problem 12.11. *Let $f(x) > 0$ be an increasing function which tends to infinity with x arbitrarily slowly. Let*

$$\mathcal{P} = \{p_n \ : \ p_{n+1} - p_n > f(n)\log n\}.$$

Show that $\#(\mathcal{P}\cap[1,x]) = o(\pi(x))$ as x tends to infinity. (Hint: Look only at primes $p \in [x/\log x, x]$. Then $f(n)\log n > g(x)\log x$, where you can take $g(x) = \frac{1}{2}f(x/\log x)$ for $x > x_0$. Now construct an interval of length $g(x)\log x$ starting at each prime in $\mathcal{P}\cap[x/\log x, x]$ and deduce that these intervals are disjoint. Hence, each such interval contains only one prime in $\mathcal{P}\cap[x/\log x, x]$. But how many disjoint intervals each of length $g(x)\log x$ can one pack in $[x/\log x, x]$?)

Problem 12.12. *Let $f(x) > 0$ be as in the preceding problem. Let*

$$\mathcal{Q} = \{p_n : p_{n+1} - p_n \le (\log n)/f(n)\}.$$

Show that $\#(\mathcal{Q} \cap [1, x]) = o(\pi(x))$ as $x \to \infty$ in the following way:

(i) *Observe that if $p \in \mathcal{Q} \cap [x/\log x, x]$, then there exists $k \le (\log x)/g(x)$ such that p and $p + k$ are both primes, where $g(x) = f(x/\log x)$.*

(ii) *Fix k. Show, using the Brun sieve, that the number of $p \le x$ such that p and $p + k$ are both primes is*

$$\ll \frac{k}{\phi(k)} \frac{x}{(\log x)^2}.$$

(iii) *Deduce that*

$$\#\left(\mathcal{Q} \cap [x/\log x, x]\right) \ll \frac{x}{(\log x)^2} \sum_{k \le (\log x)/g(x)} \frac{k}{\phi(k)}.$$

(iv) *Use the fact that $k/\phi(k) \ll \sigma(k)/k$ and Problem 7.2 to conclude that the estimate*

$$\sum_{k \le y} \frac{k}{\phi(k)} \ll y$$

holds for all $y \ge 1$.

(v) *Use (iv) with $y = (\log x)/g(x)$ in the conclusion of (iii) to conclude that $\#(\mathcal{Q} \cap [x/\log x, x]) \ll \pi(x)/g(x) = o(\pi(x))$ as $x \to \infty$.*

Problem 12.13. *Repeat Problem 12.6 but this time using Brun's combinatorial sieve instead of the pure sieve to show that the inequality asserted at (ii) holds without the factor $(\log\log x)^k$. (Hint: Show that instead of stopping with the sieving parameter y at $y = \exp(\log x/10k \log\log x)$, we can stop at $y = x^{1/ku}$, where u is absolute.) Compare your answer with the Bateman-Horn conjectures (see page 35).*

Problem 12.14. *Reconsider Problem 12.6 but now deduce that if $\nu(p) < p$ for all p, then there exists a number t, which depends on k, but not on a_i and b_i for $i = 1, \ldots, k$, such that there exist infinitely many positive integers n with $\omega(L_i(n)) \le t$ for all $i = 1, \ldots, k$. (Hint: Use the Brun sieve as a lower bound sieve and show that the main term is > 0 and dominates the error term if we sieve with $y = x^{1/ku}$. Then deduce that one can take $t = ku - 1$.) Note that, for $k = 2$ and $L_1(n) = n$, $L_2(n) = n + 2$, Brun showed that one can take $t = 9$.*

Problem 12.15. *Let $\mathcal{T}(x, y) = \{n \in [x, x + y] \ : \ n \text{ is powerful}\}$. Show that $\#\mathcal{T}(x, y) = o(y)$ as $y \to \infty$ uniformly in x. (Hint: Organize the powerful numbers $n \in [x, x + y]$ in two groups, the ones coprime to all primes $q \in [\log y, y]$ and the ones divisible by a prime in that interval. For*

the first set, use the Brun sieve to conclude that the number of such numbers is $\ll y\prod_{\log y\le p\le y}(1-1/p)\ll y\log\log y/\log y=o(y)$ *as* $y\to\infty$ *regardless of* x*. For the second group, note that if* $q\mid n$ *then* $q^2\mid n$ *since* n *is powerful. Deduce that for a fixed* q*, the number of such* n *is at most* y/q^2+1*. Now sum up over all the primes* $q\in[\log y,y]$*.)*

Problem 12.16. *Regarding the preceding problem, show that the abc conjecture implies that* $\#\mathcal{T}(x,y)\le 2$ *if* x *is large. (Hint: Assume that* $1\le i_1<i_2\le y$ *are such that* n*,* $n+i_1$ *and* $n+i_2$ *are powerful and apply the abc conjecture to the equation* $(n+i_1)(n+i_2)-n^2=(i_1+i_2)n+i_1i_2$ *to deduce that* n *is bounded in terms of* y*.) Deduce that if* $1=a_1<a_2<\cdots$ *is the increasing sequence of all the powerful numbers, then the abc conjecture implies that* $a_{n+2}-a_n\to\infty$*. Does* $a_{n+1}-a_n$ *tend to infinity? (Hint: The answer is NO and can be inferred by using Problem* 12.4*.)*

Problem 12.17. *Let* $\mathcal{P}=\{p\ :\ p+1=\phi(n)$ *for some positive integer* $n\}$*. Show that*

$$\sum_{p\in\mathcal{P}}\frac{1}{p}<\infty$$

using the following steps.

(i) *Let* x *be large. If* $p+1=\phi(n)$*, show that* $n<c_0x\log\log x:=x_1$*. (Hint: Use the minimal order of the Euler function.)*

(ii) *Let* $v=\left\lfloor\frac{1}{2}\log\log x\right\rfloor$*. If* $\omega(n)>v$*, deduce that* $2^{v-1}\mid p+1$ *and apply the Brun-Titchmarsh theorem to deduce that the number of such primes* p *is*

$$\ll x/(2^v\log(x/2^v))\ll x/(\log x)^{c_1},$$

where $c_1=1+\frac{1}{2}\log 2>1$*.*

(iii) *Let* $z=10\log\log x$*, put* $y=x_1^{1/z}$ *and use Theorem* 9.5 *to deduce that if* $p+1=\phi(n)$ *for some* n *with* $P(n)<y$*, then the number of such* p *is at most* $\Psi(x_1,y)\le x_1/\exp(u/2)\ll x/(\log x)^{c_2}$*, where one can take* $c_2=4$*. (Hint: Note that* $u=z$*.)*

(iv) *If* p *is a prime not accounted at (ii) or at (iii), then* $p+1=(q-1)\phi(m)$ *for some positive integer* $m<x_1/y$ *with* $\omega(m)\le v$*. Interpret this as saying that* $q\le x_1/\phi(m)$ *is some prime such that* $\phi(m)q+(\phi(m)+1)=p$ *is also a prime. Now use the Brun sieve to show that the number of such* q *is*

$$\ll\frac{x_1}{\phi(m)}\left(\frac{T(m)}{\phi(T(m))}\right)\frac{1}{(\log(x/\phi(m)))^2},$$

where $T(m)=\phi(m)(\phi(m)+1)$*.*

(v) *Use the minimal order of the Euler function to deduce that both inequalities*

$$T(m)/\phi(T(m)) \ll \log\log x \quad \text{and} \quad x/\phi(m) \geq x/m \gg y/\log\log x$$

hold. Infer that the last upper bound at (iv) is bounded as

$$\ll \frac{x(\log\log x)^4}{(\log x)^2}\frac{1}{\phi(m)}.$$

(vi) *Use the multinomial coefficient approach to deduce that*

$$\sum_{\substack{m\leq x\\ \omega(m)\leq v}} \frac{1}{\phi(m)} \leq \sum_{k\leq v}\frac{1}{k!}\left(\sum_{p\leq x}\frac{1}{p-1}+O(1)\right)^k \ll \left(\frac{e\log\log x+O(1)}{v}\right)^v.$$

(vii) *Deduce that the number of primes p not accounted at (ii) or (iii) but such that $p+1=\phi(n)$ is $\ll x/(\log x)^{c_3+o(1)}$ as $x\to\infty$, where* $c_3 = 2-\frac{1}{2}\log(2e) > 1$.

(viii) *Conclude.*

Problem 12.18. *Note that $p-1=\phi(p)=\phi(2p)$ if $p>2$. Let $\mathcal{P}=\{p \,:\, p-1=\phi(n)$ has at least 3 solutions $n\}$. Prove that*

$$\sum_{p\in\mathcal{P}}\frac{1}{p}<\infty.$$

(Hint: Follow the same approach as for Problem 12.17*.)*

Problem 12.19. *Adapt the argument used in the proof of Theorem* 12.9 *to show that there exists $\delta<1$ such that*

$$\#\{p\leq x \,:\, P((p-1)(p+1))<x^\delta\} \gg \frac{x}{\log x}.$$

Problem 12.20. *Adapt the proof of Proposition* 8.7 *(or Problem* 8.9*) to show that there exists a constant $c_0>0$ such that*

$$\#\{n\leq x \,:\, \phi(n) \text{ is a perfect square}\} \geq x^{c_0}$$

if $x>x_0$. (Hint: Let y be some parameter and δ the number appearing in Theorem 12.9*. Let $\mathcal{P}$ be the set of primes $p\in[y/\log y, y]$ such that $P(p-1)<p^\delta$. Choose subsets S of such primes p of exactly $\lfloor p^\delta\rfloor$ elements and let $n_S=\prod_{p\in S}p$. Then $\phi(n_S)=u_S v_S^2$, where $P(u_S)\leq y^\delta$ so that u_S can take only at most $2^{\pi(y^\delta)}$ values. Now use the Pigeon Hole principle as in the proof of Proposition* 8.7 *to get a lower bound for the number of squarefree numbers n made up of primes from $\mathcal{P}$ for which $\phi(n)$ is a square and compare this lower bound with $x=y^{y^\delta}$, which is the upper bound for such n's.)*

Problem 12.21. *Show that the same conclusion as in the preceding problem is valid if one replaces $\phi(n)$ either by $\sigma(n)$ or by $\phi(n)\sigma(n)$.*

Problem 12.22. *Let*

$$p_a(n) = \frac{1}{\omega(n)} \sum_{p|n} p$$

be the average prime factor of n. Use Vinogradov's three primes theorem (Theorem 12.18) to show that there exist infinitely many squarefree composite positive integers n for which $p_a(n)$ is a prime factor of n. For example, $105 = 3 \times 5 \times 7$ and the average of $3, 5, 7$ is 5 which is a prime factor of 105. (Hint: Let r be a large prime. Apply Vinogradov's theorem to $3r$ to deduce that there are many triples (p_1, p_2, p_3) such that $3r = p_1 + p_2 + p_3$. Then use an analogue of Theorem 12.10 to show that most of those representations have $p_i \neq p_j$ and $p_i \neq r$. Then choose $n = rp_1p_2p_3$.)

Problem 12.23. *Let $\beta(n) = \sum_{p \mid n} p$. Construct infinitely many squarefree composite integers n such that $\beta(n) \mid n$. For example, $\beta(30) = 2 + 3 + 5 = 10 \mid 30$ is such a number. (Hint: Apply an argument similar to the one used in Problem 12.22 to deduce the existence of equations of the form $r - 2 = p_1 + p_2 + p_3$, where r is a large prime and p_1, p_2, p_3 are odd distinct primes. Then look at $n = 2rp_1p_2p_3$.)*

Problem 12.24. *First show that $\sigma(\sigma(p))/p \geq 3/2$ for all primes p. Then use Chen's theorem (Theorem 12.11) to deduce that $\{\sigma(\sigma(p))/p : p \text{ prime}\}$ is dense in $[3/2, \infty)$. (Hint: Let a be an odd integer. Use the Chen Theorem to conclude that there are arbitrarily large primes p with $(p+1)/(2a)$ either a prime or a product of two large primes. Deduce that $\sigma(\sigma(p))/p = (3/2)(\sigma(a)/a)(1 + o(1))$ as $p \to \infty$ over such primes and conclude using known results about the numbers $\sigma(a)/a$ as a runs through the odd positive integers.)*

Problem 12.25. *Show that the set of positive integers n such that $p_a(n) \in \mathbb{Z}$, where p_a is defined above in Problem 12.22, is of asymptotic density zero.*

(i) *Let x be large and $n \leq x$. Argue that one may assume that $P(n) > x^{1/u}$, where $u = \log\log\log x$, that $P(n) \| n$, and that $\omega(n) \in [y - y^{2/3}, y + y^{2/3}]$, where $y = \log\log x$. Problem 7.12 might prove to be of interest.*

(ii) *Write $n = mp$, where $p = P(n)$ and $m < x/x^{1/u}$. Fix m. Then $p_a(n) \in \mathbb{Z}$ means that $p \equiv -\beta(m) \pmod{\omega(m)+1}$ and $p \leq x/m$. Use Brun-Titchmarsh (check first that it is applicable) to conclude that the number of such choices for p is*

$$\ll \frac{x}{m\phi(\omega(m)+1)} \frac{1}{\log(x/m(\omega(m)+1))}.$$

(iii) *Show that* $\log(x/(m(\omega(m)+1))) \gg (\log x)/u$ *for large* x *and then use the minimal order of the Euler function for numbers close to* y *to conclude that the bound shown at (ii) is*

$$\ll \frac{x(\log\log\log x)^2}{m\omega(m)\log x}.$$

(iv) *Sum up over* m *to conclude that the number of such integers* $n \le x$ *is*

$$\ll \frac{x(\log\log\log x)^2}{\log x}\left(\sum_{m\le x}\frac{1}{m}\right)\left(\sum_{y-y^{2/3}\le k\le y+y^{2/3}}\frac{1}{k}\right)$$

and use the calculation done at the end of Problem 7.12 *to show that the above bound is*

$$\ll \frac{x(\log\log\log x)^2}{(\log\log x)^{1/3}} = o(x) \qquad \text{as } x\to\infty.$$

Problem 12.26. *Positive integers* n *with* $\beta(n)=\beta(n+1)$ *are called Ruth-Aaron numbers (recall that* $\beta(n)=\sum_{p\mid n}p$*). One can check that* $n=714$ *is such a number. It is not known if there are infinitely many such numbers* n*. Do you have an heuristic? What does your heuristic predict? You should back it up with known conjectures such as the abc conjecture or Schinzel's Hypothesis H.*

Problem 12.27. *Show that for all* $2\le y\le x$*,*

$$\#\{n\le x \ : \ pq\mid n \text{ for some primes } y\le p<q<p\log p\} \ll \frac{x\log\log y}{\log y}.$$

(Hint: Note that if $y\le p\le q\le p\log p$*, then the number of* n *which are multiples of* pq *is* $\le x/pq$*. Then use Mertens' estimate to show that for fixed* p*,*

$$\sum_{p\le q\le p\log p}\frac{1}{q} = \log\log(p\log p)-\log\log p+O\left(\frac{1}{\log p}\right)\ll\frac{\log\log p}{\log p}.$$

It then remains to estimate

$$\sum_{p\ge y}\frac{\log\log p}{p\log p}$$

which can be done using Abel's summation formula and the Prime Number Theorem to finally conclude that it is $\ll(\log\log y)/\log y$*).*

Problem 12.28. *Show that the Ruth-Aaron numbers introduced in Problem* 12.26 *form a set of asymptotic density zero in the following way:*

(i) *Let x be large. Argue that one may assume that none of n is not $x^{1/u}$-smooth where $u = \log\log x$, that $P(n)\|n$ and that if $P_2(n)$ is the second largest prime factor of n, then $P(n) > P_2(n)(\log x)^3$ and that the same is true for $n+1$.*

(ii) *Let p and q be the largest prime factors of n and $n+1$ respectively. Deduce from $\beta(n) = \beta(n+1)$ and (i) above that $|p-q| < p/(\log x)^2$ if $x > x_0$.*

(iii) *If $pq \le x$, then the number of $n \le x$ such that $p \mid n$ and $q \mid n+1$ is $\le x/pq + 1 \le 2x/pq$. Now sum up over all pairs of primes p, q larger than $x^{1/u}$ with $|p-q| = O(p/(\log x)^2)$.*

(iv) *Write $n = pa$, $n+1 = qb$. If $pq > x$, deduce that $ab \le x$ and $|a-b| \ll a/(\log x)^2$.*

(v) *For fixed a and b with $ab \le x$, there are at most $x/ab + 1 \le 2x/ab$ positive integers $n \le x$ such that $a \mid n$ and $b \mid n+1$.*

(vi) *Show that for fixed a,*

$$\sum_{a<b<a+O(a/(\log x)^2)} \frac{1}{b} \ll \int_a^{a+O(a/(\log x)^2)} \frac{dt}{t} \ll \frac{1}{(\log x)^2}.$$

(vii) *Conclude that the number of Ruth-Aaron numbers $n \le x$ with $ab \le x$ is*

$$\ll \frac{x}{(\log x)^2} \sum_{a \le x} \frac{1}{a} \ll \frac{x}{\log x} = o(x) \qquad \text{as } x \to \infty.$$

Problem 12.29. *For an odd d, let t_d be the multiplicative order of 2 modulo d. Show that*

$$\sum_{d \text{ odd}} \frac{1}{dt_d} < \infty.$$

(Hint: Go through the proof of Proposition 9.11 and read off the fact that all odd $n \le x$ have $t_n > (\log x)^2$ except for a possible number of exceptions of cardinality $O(x/(\log x)^2)$. Hence, the odd n's with $t_n < (\log n)^2$ form a set whose counting function is $O(x/(\log x)^2)$ so that the sum of their reciprocals converges, while for the remaining n's we have $1/(nt_n) \le 1/(n(\log n)^2)$, and the series of general term $1/(n(\log n)^2)$ converges.)

Problem 12.30. *Let $r(n) = \#\{(p,k) \ : \ n = p + 2^k\}$.*

(i) *Show that*

$$\sum_{n \le x} r(n) \gg x.$$

(ii) *Show that*

$$\sum_{n \le x} r(n)^2 = \#\{(p_1,k_1,p_2,k_2) \ : \ p_1 + 2^{k_1} = p_2 + 2^{k_2}\}.$$

If $k_1 = k_2$, then $p_1 = p_2$, implying that the number of such diagonal quadruples (p_1, k_1, p_2, k_2) is $\le \pi(x)(\log x/\log 2) \ll x$.

(iii) *Show, using the Brun sieve, that the number of nondiagonal quadruples is*

$$\sum_{k\le \log x/\log 2} \frac{x}{\log x} \prod_{p\mid 2^k-1}\left(1+\frac{1}{p}\right) \ll \frac{x}{\log x}\sum_{\substack{d\le x\\ d\ odd}}\frac{1}{d}\sum_{\substack{k\le \log x/\log 2\\ t_d\mid k}} 1$$
$$\ll \frac{x}{\log x}\sum_{d\ odd}\frac{\log x}{dt_d},$$

where t_d is the multiplicative order of 2 modulo d, and now use Problem 12.29 *to conclude that $\sum_{n\le x} r(n)^2 \ll x$.*

(iv) *Use the Cauchy-Schwarz inequality as in the proof of Theorem* 12.17 *to show that the set of numbers $n = p + 2^k$ has positive lower asymptotic density. (Yet remember that its complement also has positive lower asymptotic density, for example from Problem* 7.20*.)*

Problem 12.31. *The aim of this problem is to show that*

$$\sum_{n\ge 1}\frac{p_n}{n!} \notin \mathbb{Q}, \tag{12.32}$$

where as usual p_n stands for the n-th prime. Assume for a contradiction that the series appearing at (12.32) *is rational.*

(i) *Using the fact that $p_n = n(\log n + O(\log\log n))$, deduce that if the number shown at* (12.32) *is rational then for each n there exist integers a and b of the size $\log n + O(\log\log n)$ such that $p_n = na - b$.*

(ii) *Use the Pigeon Hole Principle to show that there exist integers a and b of the sizes shown in (i) such that $p_k = ka - b$ holds for a set of $k \in [n, 2n]$ of cardinality $\gg n/(\log\log n)^2$.*

(iii) *Use the Brun-Tichmarsh theorem to get an upper bound on the set of primes $p \in [p_n, p_{2n}]$ which are congruent to $-b \pmod a$. Can you see that you reached a contradiction?*

Problem 12.32. *The number $n = 113$ has the property that if we delete any of its digits, the number that remains is prime. Show that the number of $n \le x$ with this property is smaller than x^c for some positive constant c as $x \to \infty$. Are there infinitely many such positive integers ?*

Problem 12.33. *Show that the Fermat number $F_m = 2^{2^m} + 1$ with $m > 0$ is prime if and only if $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$. This result is known as Pépin's test, named after the French mathematician Théophile Pépin who discovered this primality test in 1877.*