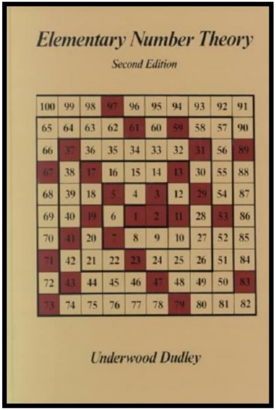
Elementary Number Theory

Section 21. Bounds for $\pi(x)$—Proofs of Theorems



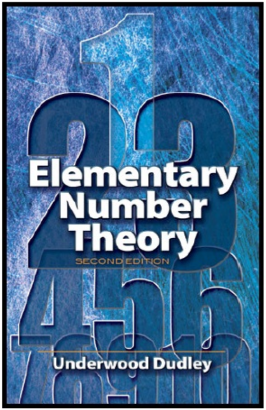


Table of contents

Lemma 21.1

Lemma 21.1. The highest power of p that divides $n!$ is $[n/p] + [n/p^2] + [n/p^3] + \cdots$.

Proof. Each *multiple* of p less than or equal to n adds one *power* of p to $n!$; there are $[n/p]$ such multiples. Each multiple of p^2 less than or equal to n adds an *additional* power of p to $n!$; there are $[n/p^2]$ such multiples (notice that p^2 is both a multiple of p and a multiple of p^2 and it is counted twice here, once in $[n/p]$ and once as $[n/p^2]$, as needed). Similarly, each multiple of p^k less than or equal to n adds an additional power of p to $n!$; there are $[n/p^k]$ such multiples. Hence p to the power $[n/p] + [n/p^2] + [n/p^3] + \cdots$ divides $n!$. (Notice that for $p^k > n$, we have $[n/p^k] = 0$, so there are no convergence concerns here and, in fact, $[n/p] + [n/p^2] + [n/p^3] + \cdots$ can be treated as a finite sum.) □

Lemma 21.1

Lemma 21.1. The highest power of p that divides $n!$ is $[n/p] + [n/p^2] + [n/p^3] + \cdots$.

Proof. Each *multiple* of p less than or equal to n adds one *power* of p to $n!$; there are $[n/p]$ such multiples. Each multiple of p^2 less than or equal to n adds an *additional* power of p to $n!$; there are $[n/p^2]$ such multiples (notice that p^2 is both a multiple of p and a multiple of p^2 and it is counted twice here, once in $[n/p]$ and once as $[n/p^2]$, as needed). Similarly, each multiple of p^k less than or equal to n adds an additional power of p to $n!$; there are $[n/p^k]$ such multiples. Hence p to the power $[n/p] + [n/p^2] + [n/p^3] + \cdots$ divides $n!$. (Notice that for $p^k > n$, we have $[n/p^k] = 0$, so there are no convergence concerns here and, in fact, $[n/p] + [n/p^2] + [n/p^3] + \cdots$ can be treated as a finite sum.) □

Lemma 21.2

Lemma 21.2 The highest power of p that divides $\binom{2n}{n}$ is

$$[2n/p] - 2[n/p] + 2[n/p^2] - 2[n/p^2] + [2n/p^3] - 2[n/p^3] + \cdots .$$

Proof. Since $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$, then we can apply Lemma 21.1 to the numerator and (twice) to the denominator. By Lemma 21.1, the numerator contains exactly $[2n/p] + [2n/p^2] + p2n/p^3] + \cdots$ factors of p. The denominator contains exactly $2([n/p] + [n/p^2] + [n/p^3] + \cdots)$ factors of p. So the quotient $(2n!)/(n!)^2$ contains the claimed number of factors of p. (Again, the sums here are effectively finite, so that rearrangement is no concern.) □

Lemma 21.2

Lemma 21.2 The highest power of p that divides $\binom{2n}{n}$ is

$$[2n/p] - 2[n/p] + 2[n/p^2] - 2[n/p^2] + [2n/p^3] - 2[n/p^3] + \cdots .$$

Proof. Since $\binom{2n}{n} = \dfrac{(2n)!}{(n!)^2}$, then we can apply Lemma 21.1 to the numerator and (twice) to the denominator. By Lemma 21.1, the numerator contains exactly $[2n/p] + [2n/p^2] + p2n/p^3] + \cdots$ factors of p. The denominator contains exactly $2([n/p] + [n/p^2] + [n/p^3] + \cdots)$ factors of p. So the quotient $(2n!)/(n!)^2$ contains the claimed number of factors of p. (Again, the sums here are effectively finite, so that rearrangement is no concern.) □

Lemma 21.3

Lemma 21.3. For any x, $[2x] - x[x] \leq 1$.

Proof. By the definition of the greatest integer function, we have $[2x] \leq 2x$ and $[x] > x - 1$ for all $x \geq 1$ (say), so $[2x] - 2[x] < 2x - 2(x - 1) = 2$. Since $[2x] - 2[x]$ is an integer, then we must in fact have $[2n] - 2[x] \leq 1$. □

Lemma 21.3

Lemma 21.3. For any x, $[2x] - x[x] \leq 1$.

Proof. By the definition of the greatest integer function, we have $[2x] \leq 2x$ and $[x] > x - 1$ for all $x \geq 1$ (say), so $[2x] - 2[x] < 2x - 2(x - 1) = 2$. Since $[2x] - 2[x]$ is an integer, then we must in fact have $[2n] - 2[x] \leq 1$. □

Lemma 21.4

Lemma 21.4. Each prime-power in the prime-power decomposition of $\binom{2n}{n}$ is less than or equal to $2n$.

Proof. Suppose p^r is in the prime-power decomposition of $\binom{2n}{n}$. ASSUME $p^r > 2n$. Then $[2n/p^r] = [2n/p^{r+1}] = \cdots = 0$ and $[n/p^r] = [n/p^{r+1}] = \cdots = 0$. So by Lemma 21.2, the highest power of p that divides $\binom{2n}{n}$ is

$$r = ([2/p] - 2[n/p]) + (2n/p^2] - 2[n/p^2]) + \cdots + ([2n/p^{r-1}] - 2[n/p^{r-1}]).$$

Lemma 21.4

Lemma 21.4. Each prime-power in the prime-power decomposition of $\binom{2n}{n}$ is less than or equal to $2n$.

Proof. Suppose p^r is in the prime-power decomposition of $\binom{2n}{n}$. ASSUME $p^r > 2n$. Then $[2n/p^r] = [2n/p^{r+1}] = \cdots = 0$ and $[n/p^r] = [n/p^{r+1}] = \cdots = 0$. So by Lemma 21.2, the highest power of p that divides $\binom{2n}{n}$ is

$$r = ([2/p] - 2[n/p]) + (2n/p^2] - 2[n/p^2]) + \cdots + ([2n/p^{r-1}] - 2[n/p^{r-1}]).$$

But by Lemma 21.3, each of the terms in parentheses is at most 1, so that $r \leq \underbrace{1 + 1 + \cdots + 1}_{r-1 \text{ times}} = r - 1$, a CONTRADICTION. So the assumption that $p^r > 2n$ is false, and hence we have $p^r \leq 2n$, as claimed. □

Lemma 21.4

Lemma 21.4. Each prime-power in the prime-power decomposition of $\binom{2n}{n}$ is less than or equal to $2n$.

Proof. Suppose p^r is in the prime-power decomposition of $\binom{2n}{n}$. ASSUME $p^r > 2n$. Then $[2n/p^r] = [2n/p^{r+1}] = \cdots = 0$ and $[n/p^r] = [n/p^{r+1}] = \cdots = 0$. So by Lemma 21.2, the highest power of p that divides $\binom{2n}{n}$ is

$$r = ([2/p] - 2[n/p]) + (2n/p^2] - 2[n/p^2]) + \cdots + ([2n/p^{r-1}] - 2[n/p^{r-1}]).$$

But by Lemma 21.3, each of the terms in parentheses is at most 1, so that $r \leq \underbrace{1 + 1 + \cdots + 1}_{r-1 \text{ times}} = r - 1$, a CONTRADICTION. So the assumption that $p^r > 2n$ is false, and hence we have $p^r \leq 2n$, as claimed. □

Lemma 21.5

Lemma 21.5. For $n \geq 1$, we have $2^n \leq \binom{2n}{n} \leq 2^{2n}$.

Proof. We give a proof using induction. For the base case, with $n = 1$ we have $\binom{2}{1} = 2$ and $2^1 \leq 2 \leq 2^{2(1)}$. For the induction hypothesis, suppose the claim holds for $n = k$ and that $2^k \leq \binom{2k}{k} \leq 2^{2k}$. Consider $n = k + 1$. We have

$$\binom{2(k+1)}{k+1} = \frac{(2k+2)!}{((k+1)!)^2} = \frac{(2k+2)(2k+1)(2k)!}{(k+1)k!(k+1)k!}$$

$$= \frac{2(k+1)(2k+1)}{(k+1)(k+1)} \frac{(2k)!}{k!k!} = \frac{2(2k+1)}{k+1} \binom{2k}{k}.$$

Lemma 21.5

Lemma 21.5. For $n \geq 1$, we have $2^n \leq \binom{2n}{n} \leq 2^{2n}$.

Proof. We give a proof using induction. For the base case, with $n = 1$ we have $\binom{2}{1} = 2$ and $2^1 \leq 2 \leq 2^{2(1)}$. For the induction hypothesis, suppose the claim holds for $n = k$ and that $2^k \leq \binom{2k}{k} \leq 2^{2k}$. Consider $n = k + 1$. We have

$$\binom{2(k+1)}{k+1} = \frac{(2k+2)!}{((k+1)!)^2} = \frac{(2k+2)(2k+1)(2k)!}{(k+1)k!(k+1)k!}$$

$$= \frac{2(k+1)(2k+1)}{(k+1)(k+1)} \frac{(2k)!}{k!k!} = \frac{2(2k+1)}{k+1} \binom{2k}{k}.$$

Lemma 21.5 (continued 1)

Lemma 21.5. For $n \geq 1$, we have $2^n \leq \binom{2n}{n} \leq 2^{2n}$.

Proof (continued). $\ldots \binom{2(k+1)}{k+1} = \frac{2(2k+1)}{k+1}\binom{2k}{k}$.

Next we have

$$\begin{aligned} \frac{2(2k+1)}{k+1}\binom{2k}{k} &< \frac{2(2k+2)}{k+1}\binom{2k}{k} \text{ since } 2k+1 < 2k+2 \\ &= 4\binom{2k}{k} \leq 4 \cdot 2^{2k} \text{ by the induction hypothesis} \\ &= 2^{2(k+1)}, \end{aligned}$$

and the upper bound holds for $n = k+1$:

$$\binom{2(k+1)}{k+1} = \frac{2(2k+1)}{k+1}\binom{2k}{k} < 2^{2(k+1)}.$$

Lemma 21.5 (continued 1)

Lemma 21.5. For $n \geq 1$, we have $2^n \leq \binom{2n}{n} \leq 2^{2n}$.

Proof (continued). $\ldots \binom{2(k+1)}{k+1} = \frac{2(2k+1)}{k+1}\binom{2k}{k}$.

Next we have

$$\begin{aligned} \frac{2(2k+1)}{k+1}\binom{2k}{k} &< \frac{2(2k+2)}{k+1}\binom{2k}{k} \text{ since } 2k+1 < 2k+2 \\ &= 4\binom{2k}{k} \leq 4 \cdot 2^{2k} \text{ by the induction hypothesis} \\ &= 2^{2(k+1)}, \end{aligned}$$

and the upper bound holds for $n = k+1$:

$$\binom{2(k+1)}{k+1} = \frac{2(2k+1)}{k+1}\binom{2k}{k} < 2^{2(k+1)}.$$

Lemma 21.5 (continued 2)

Lemma 21.5. For $n \geq 1$, we have $2^n \leq \binom{2n}{n} \leq 2^{2n}$.

Proof (continued). $\ldots \binom{2(k+1)}{k+1} = \frac{2(2k+1)}{k+1}\binom{2k}{k}$. Similarly,

$$\begin{aligned} \frac{2(2k+1)}{k+1}\binom{2k}{k} &> \frac{2(k+1)}{k+1}\binom{2k}{k} \text{ since } 2k+1 > k+1 \\ &= 2\binom{2k}{k} \geq 2 \cdot 2^{2k} \text{ by the induction hypothesis} \\ &= 2^{k+1}, \end{aligned}$$

and the lower bound holds for $n = k+1$:

$$\binom{2(k+1)}{k+1} = \frac{2(2k+1)}{k+1}\binom{2k}{k} > 2^{k+1}.$$

Therefore, by induction, the bound holds for all $n \geq 1$, as claimed. □

Lemma 21.6

Lemma 21.6. For $n \geq 2$, we have $\pi(2n) - \pi(n) \leq (2n \log 2)/\log n$.

Proof. Because $\binom{2n}{n} = \dfrac{(2n)(2n-1)\cdots(n+1)}{n(n-1)\cdots(2)(1)}$, the prime power decomposition of $\binom{2n}{n}$ contains each prime strictly between n and $2n$ (since these primes appear in the numerator and cannot be canceled by any factor in the denominator). Thus (since $2n$ is not prime)

$$\binom{2n}{n} \geq \prod_{n<p<2n} p = \prod_{n<p\leq 2n} p.$$

Lemma 21.6

Lemma 21.6. For $n \geq 2$, we have $\pi(2n) - \pi(n) \leq (2n \log 2)/\log n$.

Proof. Because $\binom{2n}{n} = \dfrac{(2n)(2n-1)\cdots(n+1)}{n(n-1)\cdots(2)(1)}$, the prime power decomposition of $\binom{2n}{n}$ contains each prime strictly between n and $2n$ (since these primes appear in the numerator and cannot be canceled by any factor in the denominator). Thus (since $2n$ is not prime)

$$\binom{2n}{n} \geq \prod_{n<p<2n} p = \prod_{n<p\leq 2n} p.$$

But each prime p in the product is strictly larger than n, so $\prod_{n<p\leq 2n} p \geq \prod_{n<p\leq 2n} n$ and, since there are $\pi(2n) - \pi(n)$ primes p satisfying $n < p \leq 2n$, then $\prod_{n<p\leq 2n} n = n^{\pi(2n)-\pi(n)}$.

Lemma 21.6

Lemma 21.6. For $n \geq 2$, we have $\pi(2n) - \pi(n) \leq (2n \log 2)/\log n$.

Proof. Because $\binom{2n}{n} = \frac{(2n)(2n-1)\cdots(n+1)}{n(n-1)\cdots(2)(1)}$, the prime power decomposition of $\binom{2n}{n}$ contains each prime strictly between n and $2n$ (since these primes appear in the numerator and cannot be canceled by any factor in the denominator). Thus (since $2n$ is not prime)

$$\binom{2n}{n} \geq \prod_{n<p<2n} p = \prod_{n<p\leq 2n} p.$$

But each prime p in the product is strictly larger than n, so $\prod_{n<p\leq 2n} p \geq \prod_{n<p\leq 2n} n$ and, since there are $\pi(2n) - \pi(n)$ primes p satisfying $n < p \leq 2n$, then $\prod_{n<p\leq 2n} n = n^{\pi(2n)-\pi(n)}$.

Lemma 21.6 (continued)

Lemma 21.6. For $n \geq 2$, we have $\pi(2n) - \pi(n) \leq (2n \log 2)/\log n$.

Proof (continued). Combining these three inequalities we have

$$\binom{2n}{n} \geq \prod_{n<p\leq 2n} p \geq \prod_{n<p\leq 2n} n = n^{\pi(2n)-\pi(n)}.$$

By Lemma 21.5, we have

$$2^{2n} \geq \binom{2n}{n} \geq n^{\pi(2n)-\pi(n)}.$$

taking logarithms of both sides gives $2n \log 2 \geq (\pi(2n) - \pi(n)) \log n$, as claimed. □

Lemma 21.7

Lemma 21.7. For $n \geq 2$, we have $\pi(2n) \geq (n \log 2)/\log(2n)$.

Proof. By Lemma 21.4, each prime-power in the prime-power decomposition of $\binom{2n}{n}$ is at most $2n$. There are most $\pi(2n)$ such prime powers, so $\binom{2n}{n} \leq (2n)^{\pi(2n)}$. By Lemma 21.5, we get $2^n \leq (2n)^{\pi(2n)}$, so taking logarithms of both sides gives $n \log 2 \leq \pi(2n) \log(2n)$, as claimed. □

Lemma 21.7

Lemma 21.7. For $n \geq 2$, we have $\pi(2n) \geq (n \log 2)/\log(2n)$.

Proof. By Lemma 21.4, each prime-power in the prime-power decomposition of $\binom{2n}{n}$ is at most $2n$. There are most $\pi(2n)$ such prime powers, so $\binom{2n}{n} \leq (2n)^{\pi(2n)}$. By Lemma 21.5, we get $2^n \leq (2n)^{\pi(2n)}$, so taking logarithms of both sides gives $n \log 2 \leq \pi(2n) \log(2n)$, as claimed. □

Lemma 21.8

Lemma 21.8. For $r \geq 1$, we have $\pi(2^{2r}) < 2^{2r+2}/r$.

Proof. We use induction. With $r = 1$ we have $\pi(2^{2(1)}) = \pi(4) = 2 < 2^{2(1)+2}/(1) = 16$, so that the base case is established. For the induction step, suppose that the lemma holds for $r = k$: $\pi(2^{2k}) < 2^{2k+2}/k$.

Lemma 21.8

Lemma 21.8. For $r \geq 1$, we have $\pi(2^{2r}) < 2^{2r+2}/r$.

Proof. We use induction. With $r = 1$ we have $\pi(2^{2(1)}) = \pi(4) = 2 < 2^{2(1)+2}/(1) = 16$, so that the base case is established. For the induction step, suppose that the lemma holds for $r = k$: $\pi(2^{2k}) < 2^{2k+2}/k$. Then for $r = k + 1$ we have

$$\begin{aligned}
\pi(2^{2(k+1)}) &= \pi(2^{2k+2}) = \pi(2 \cdot 2^{2k+1}) \\
&\leq \frac{2(2^{2k+1}) \log 2}{\log 2^{2k+1}} + \pi(2^{2k+1}) \text{ by Lemma 21.6 with } n = 2^{2k+1} \\
&= \frac{2^{2k+2} \log 2}{(2k+1) \log 2} + \pi(2^{2k+1}) = \frac{2^{2k+2}}{2k+1} + \pi(2 \cdot 2^{2k}) \\
&\leq \frac{2^{2k+2}}{2k+1} + \frac{2(2^{2k}) \log 2}{\log 2^{2k}} + \pi(2^{2k}) \text{ by Lemma 21.6} \\
&\quad \text{with } n = 2^{2k}
\end{aligned}$$

Lemma 21.8

Lemma 21.8. For $r \geq 1$, we have $\pi(2^{2r}) < 2^{2r+2}/r$.

Proof. We use induction. With $r = 1$ we have $\pi(2^{2(1)}) = \pi(4) = 2 < 2^{2(1)+2}/(1) = 16$, so that the base case is established. For the induction step, suppose that the lemma holds for $r = k$: $\pi(2^{2k}) < 2^{2k+2}/k$. Then for $r = k + 1$ we have

$$\begin{aligned}
\pi(2^{2(k+1)}) &= \pi(2^{2k+2}) = \pi(2 \cdot 2^{2k+1}) \\
&\leq \frac{2(2^{2k+1}) \log 2}{\log 2^{2k+1}} + \pi(2^{2k+1}) \text{ by Lemma 21.6 with } n = 2^{2k+1} \\
&= \frac{2^{2k+2} \log 2}{(2k+1) \log 2} + \pi(2^{2k+1}) = \frac{2^{2k+2}}{2k+1} + \pi(2 \cdot 2^{2k}) \\
&\leq \frac{2^{2k+2}}{2k+1} + \frac{2(2^{2k}) \log 2}{\log 2^{2k}} + \pi(2^{2k}) \text{ by Lemma 21.6} \\
&\quad \text{with } n = 2^{2k}
\end{aligned}$$

Lemma 21.8 (continued 1)

Lemma 21.8. For $r \geq 1$, we have $\pi(2^{2r}) < 2^{2r+2}/r$.

Proof (continued). ...

$$\begin{aligned}
\pi(2^{2(k+1)}) &\leq \frac{2^{2k+2}}{2k+1} + \frac{2(2^{2k})\log 2}{\log 2^{2k}} + \pi(2^{2k}) \\
&< \frac{2^{2k+2}}{2k+1} + \frac{2^{2k+1}}{2k} + \frac{2^{2k+2}}{k} \text{ by the induction hypothesis} \\
&= \frac{2^{2k+2}}{2k+1} + \frac{2^{2k}}{k} + \frac{2^{2k+2}}{k} \\
&< \frac{2^{2k+2}}{2k} + \frac{2^{2k}}{k} + \frac{2^{2k+2}}{k} \text{ since } \frac{1}{2k+1} < \frac{1}{2k} \\
&= \frac{2^{2k+1} + 2^{2k} + 2^{2k+2}}{k} = \frac{3 \cdot 2^{2k} + 2^{2k+2}}{k}
\end{aligned}$$

Lemma 21.8 (continued 2)

Lemma 21.8. For $r \geq 1$, we have $\pi(2^{2r}) < 2^{2r+2}/r$.

Proof (continued). ...

$$\begin{aligned}
\pi(2^{2(k+1)}) &< \frac{2^{2k+1} + 2^{2k} + 2^{2k+2}}{k} = \frac{3 \cdot 2^{2k} + 2^{2k+2}}{k} \\
&\leq \frac{3 \cdot 2^{2k} + 2^{2k+2}}{k} \frac{2k}{k+1} \text{ since } 1 \leq \frac{2k}{k+1} \text{ for } k \geq 1 \\
&= \frac{3 \cdot 2^{2k+1} + 2^{2k+3}}{k+1} < \frac{4 \cdot 2^{2k+1} + 2^{2k+3}}{k+1} \\
&= \frac{2^{2k+3} + 2^{2k+3}}{k+1} = \frac{2^{2k+4}}{k+1} = \frac{2^{2(k+1)+2}}{k+1}.
\end{aligned}$$

So the claim holds for $r = k + 1$ and, by induction, holds for all integers $r \geq 1$, as claimed. □

Theorem 21.1

Theorem 21.1. For $x \geq 2$, we have
$$\frac{1}{4}\log 2(x/\log x) \leq \pi(x) \leq (32\log 2)(x/\log x).$$

Proof. For the lower bound, fix x and let n be so that $2n \leq x < 2n+2$. We have

$$\begin{aligned}
\pi(x) &\geq \pi(2n) \text{ since } \pi(x) \text{ is an increasing function} \\
&\geq \frac{n\log 2}{\log(2n)} \text{ by Lemma 21.7} \\
&\geq \frac{n\log 2}{\log x} \text{ since } 2n \leq x \text{ so that } \log(2n) \leq \log x \\
&\geq \frac{2n+2}{4}\frac{\log 2}{\log x} \text{ since } n \geq \frac{2n+2}{4} \text{ for } n \geq 1 \\
&> \frac{x}{4}\frac{\log 2}{\log x} \text{ since } 2n+2 > x.
\end{aligned}$$

Theorem 21.1

Theorem 21.1. For $x \geq 2$, we have

$$\frac{1}{4}\log 2(x/\log x) \leq \pi(x) \leq (32\log 2)(x/\log x).$$

Proof. For the lower bound, fix x and let n be so that $2n \leq x < 2n+2$. We have

$$\begin{aligned}
\pi(x) &\geq \pi(2n) \text{ since } \pi(x) \text{ is an increasing function} \\
&\geq \frac{n\log 2}{\log(2n)} \text{ by Lemma 21.7} \\
&\geq \frac{n\log 2}{\log x} \text{ since } 2n \leq x \text{ so that } \log(2n) \leq \log x \\
&\geq \frac{2n+2}{4}\frac{\log 2}{\log x} \text{ since } n \geq \frac{2n+2}{4} \text{ for } n \geq 1 \\
&> \frac{x}{4}\frac{\log 2}{\log x} \text{ since } 2n+2 > x.
\end{aligned}$$

Theorem 21.1 (continued)

Theorem 21.1. For $x \geq 2$, we have

$$\frac{1}{4}\log 2(x/\log x) \leq \pi(x) \leq (32\log 2)(x/\log x).$$

Proof (continued). For the upper bound, fix x and let r be so that $2^{2r-2} \leq x < 2^r$. We have

$$\begin{array}{rcll} \dfrac{\pi(x)}{x} & \leq & \dfrac{\pi(2^{2r})}{x} & \text{since } \pi(x) \text{ is an increasing function} \\ & \leq & \dfrac{\pi(2^{2r})}{2^{2r-2}} & \text{since } 2^{2r-2} \leq x \\ & < & \dfrac{2^{2r+2}}{2^{2r-2}r} & \text{by Lemma 21.8} \\ & = & 16/r. & \end{array}$$

Since $x < 2^{2r}$ then $\log x < \log(2^{2r}) = 2r\log 2$, and $1/r < (2\log 2)/(\log x)$. Therefore $\dfrac{\pi(x)}{x} < \dfrac{16}{r} < \dfrac{32\log 2}{\log x}$, as claimed. □