Theorem 36 $p_n < 2^{2^n}$, for every $n$ and so $\pi(m) > \ln \ln m$, when $m = 2^{2^n}$.

Proof: We’ll use induction on $n$. First $p_1 = 2 < 2^{2^1} = 4$ and so the result is true for $n = 1$. Suppose that $p_k < 2^{2^k}$ for $k = 1, 2, \ldots, n$ and consider $p_{n+1}$. The argument of Theorem 35 shows that $p_{n+1} \leq p_1 p_2 \ldots p_n + 1$ and so

\[
p_{n+1} \leq p_1 p_2 \ldots p_n + 1 < 2^{1} 2^{2} \ldots 2^{2^n} + 1, \text{ by induction}
\]

\[
= 2^{2+4+\ldots+2^n} + 1
\]

\[
= 2^{(2^n-1)} + 1
\]

\[
< 2^{2^{n+1}}.
\]

The result follows by induction for all $n$.

It follows that the $n$–th prime is at most $2^{2^n}$ and this implies that $\pi(2^{2^n}) \geq n$. Since $\ln(2^{2^n}) = 2^n \ln 2 < 2^n$, we have

\[
\ln \ln(2^{2^n}) < n \ln 2 < n \leq \pi(2^{2^n}).
\]

This completes the proof.

Hence $\pi(m) \geq \ln \ln m$ when $m$ has the form $m = 2^{2^m}$. This is not actually an amazing result. For example, when $n = 4$, it is asserting that $\pi(2^{16}) = 2.406 \ldots > 2$ and there are more than 2 primes less than 65536. Not a huge discovery! On the other hand it is giving an estimate for the number of primes less than $2^{2^n}$ which goes to infinity and $n$ goes to infinity, however slow and inaccurate the estimate is.

It was the famous Prime Number Theorem proved in 1896 by Hadamard and De le Vallée Poussin, which showed that when $n$ is large $\pi(n)$ is approximately $\frac{n}{\ln n}$, a result conjectured by Gauss after intensive calculation of primes.

In fact Theorem 36 shows that $\pi(x) > \ln \ln x$ for every $x$ and not just integers $2^{2^n}$. I will include the proof of this on the website but won’t give it here in class.

For suppose that we choose $n \geq 4$ so that $e^{e^{n-1}} < x \leq e^{e^n}$. Then $e^{e^{n-1}} > 2^{n}$ and $e^{e^{n-1}} > 2^{2^n}$.

Thus

\[
\pi(x) \geq \pi(e^{e^{n-1}}) \geq \pi(2^{2^n}) \geq n \geq \ln \ln x.
\]

Hence we have
Theorem 36a $\pi(x) > \ln \ln x$, for $x > e^{e^2}$.

We can adapt Theorem 35 in a number of ways. There are two kinds of primes, even ones (or better one even one, 2) and odd primes. The odd primes come in two varieties, because when you divide an odd number by 4, the remainder is either 1 or 3.

\[
\begin{align*}
1 & \pmod{4} \\
3 & \pmod{4}
\end{align*}
\]

13 17 29 37 43 53 61 73 89 97 \ldots

3 7 11 19 23 31 43 47 59 67 71 83 \ldots

Of course it would be a brave suggestion if I were to say that I have written down all the primes $\equiv 1 \pmod{4}$ or $\equiv 3 \pmod{4}$ here - and I haven’t! In fact, there are infinitely many primes in each list. Surprisingly it is easier to prove one rather than the other:

**Theorem 37** There are infinitely many primes $p \equiv 3 \pmod{4}$.

**Proof.**

Suppose that $p_1, p_2, \ldots, p_n$ are primes $\equiv 3 \pmod{4}$. Then consider $N = 4p_1p_2 \ldots p_n - 1$.

First $N$ is clearly odd and must be divisible by some odd prime. It is also not divisible by any of the primes $p_1, p_2, \ldots p_n$ because if for example $p_1 | N$ then $p_1 | N - 4p_1p_2 \ldots p_n = -1$.

On the other hand $N$ cannot be divisible only by primes $p \equiv 1 \pmod{4}$, because the product of primes $\equiv 1 \pmod{4}$ is itself $\equiv 1 \pmod{4}$ while $N \equiv 3 \pmod{4}$. Hence $N$ must be divisible by a prime $p \equiv 3 \pmod{4}$, where $p \neq p_i$, for $i = 1, 2, \ldots, n$.

Hence there are infinitely many primes $\equiv 3 \pmod{4}$.

This completes the proof.

The similar adaptation for the case $\equiv 1 \pmod{4}$ does not work, because the corresponding number $N = 4p_1p_2 \ldots p_n + 1$ might be divisible only by primes $p \equiv 3 \pmod{4}$. (For example, the number $4.5.17 + 1 = 11.31$.)

However the result is still true:

**Theorem 38** There are infinitely many primes $p \equiv 1 \pmod{4}$.

**Proof**

Suppose that $p_1, p_2, \ldots p_n$ are primes $\equiv 1 \pmod{4}$. Consider $N = 4p_1^2p_2^2 \ldots p_n^2 + 1$.

Again $N$ is odd and so is divisible only by odd primes. It is not divisible by any of the primes $p_1, p_2, \ldots p_n$ because if for example $p_1 | N$ then $p_1 | N - 4p_1^2p_2^2 \ldots p_n^2 = 1$.

On the other hand $N = x^2 + 1 \not\equiv 0 \pmod{p}$, when $p \equiv 3 \pmod{4}$ with $x = 2p_1p_2 \ldots p_n$, by Theorem 28.

Hence $N$ is divisible by some prime $p \equiv 1 \pmod{4}$, different from $p_1, p_2, \ldots, p_n$.

This completes the proof.

I want to leave primes in arithmetic progressions for a bit and to go down a different route. We have shown that there are infinitely many primes in each of the sequences $\{4n + 1\}$ and $\{4n + 3\}$. Exercises will show a few more examples in the tutorial. It turns out that there are infinitely many primes in any arithmetic sequence $\{an + b\}$ when $(a, b) = 1$. This is a
famous and difficult result of Dirichlet from 1837, a result which uses difficult complex analysis surprisingly enough.

RETURN TO $Z[i]_{2+3i}$

There was a serious problem with $Z[i]_{2+3i}$ which I deliberately avoided telling you about. The possible remainders in this ring are the Gaussian integers of norm at most $\frac{13}{2}$. They are

$$0, \pm 1, \pm i, \pm 1 \pm i, \pm 2, \pm 2i, \pm 1 \pm 2i, \pm 2 \pm i$$

There are 21 elements here. What I neglected to observe in that collection is that they are not all different modulo $2 + 3i$. For example $2 + i = -2i \pmod{2 + 2i}$.

This is a serious matter. It would be as if I had begun in the first lecture with $Z_7$ and told you that the elements of this ring are

$$0, 1, 2, 3, 4, 5, 6, 133, -11$$

Calculation would be confused completely. So there are fewer than 21 elements in this ring, and it is not at the moment clear how many elements there actually are.

To see this I want us to mark into the complex plane the Gaussian integer points and the Gaussian integer multiples of $2 + 3i$.

****

Every Gaussian integer can be moved to a unique Gaussian integer into $OABC$ or onto the vertices of the square $OABC$ by shifts parallel to $2 + 3i$ and $-3 + 2i$. That is, every Gaussian integer is congruent modulo $2 + 3i$ to exactly one of the following:

$$0, -1 + i, -2 + 2i, -1 + 2i, 2i, 1 + 2i, -2 + 3i, -1 + 3i, 3i, 1 + 3i, -1 + 4i, 4i$$

Note that the vertices $0, 2 + 3i, -3 + 2i, -1 + 5i$ are all congruent to 0 modulo $2 + 3i$.

There are 13 elements in this ring. Lest some of you feel that this collection of remainders involves elements whose norm is larger than $\frac{13}{2}$, don’t worry! If you are desperate you can write each of these numbers congruent to an element of $Z[i]_{2+3i}$ of norm $\leq 6\frac{1}{2}$ - but you don’t want to!! These elements are definitely different modulo $2 + 3i$ and every Gaussian integer is congruent to a unique one of them!

Calculation in the ring is still difficult, unfortunately. For example, what is $(-2 + 3i)(-1 + 2i)$? Well, it is $-4 - 7i$, which is not in our set. We need to shift it into the square $OABC$ by legal shifts.

$$-4 - 7i \equiv -4 - 8i + 3(2 + 3i) + 1(-3 + 2i)$$

$$\equiv -1 + 4i,$$

an element in our set of remainders. So $(-2 + 2i)(-1 + 3i) = -1 + 4i \in Z[i]_{2+3i}$.

It is still a very unsatisfactory situation. Calculation is still difficult. Presumably we still don’t know what the units are!

I want to leave this topic here for you to think about for a while.