1. a) Let $z, q \in \mathbb{Z}[j]$, then $z/q \in \mathbb{Q}(j) = \mathbb{Q}(\mathrm{i}\sqrt{3})$, so we write it as $z/q = x + \mathrm{i}\sqrt{3}y$. Let $a, b \in \mathbb{Z}$ such that $|x - a| \leqslant 1/2$ and $|y - b| \leqslant 1/2$. If $|x - a| < 1/2$ or $|y - b| < 1/2$, then we obtain
$$|z/q - (a + \mathrm{i}\sqrt{3}b)|^2 = (x - a)^2 + 3(y - b)^2 < 1.$$
Hence we choose $r = z - zq$. If $|x - a| = |y - b| = 1/2$, then $z/q \in \mathbb{Z}[j]$ and we take $r = 0$. This proves that $\mathbb{Z}[j]$ is an Euclidean ring.

   b) We have
$$(\alpha) = (a + bj)(\mathbb{Z} + j\mathbb{Z}) = \mathbb{Z}(a + bj) + \mathbb{Z}(aj - b - bj).$$
The index of (α) in $\mathbb{Z}[j]$ is the index of $\mathbb{Z}(a, b) + \mathbb{Z}(-b, a - b)$ in $\mathbb{Z}^2 = \mathbb{Z}(1, 0) + \mathbb{Z}(0, 1)$ which is equal to
$$\left|\det \begin{pmatrix} a & -b \\ b & a - b \end{pmatrix}\right| = a^2 - ab + b^2.$$

   c) Observe that in general, if $f : A \to B$ is a surjective ring homomorphism, $J \subseteq B$ an ideal and $I \subseteq A$ an ideal is such that $f(I) = J$, we have $f^{-1}(J) = I + \ker f$. Now consider the composition
$$\mathbb{Z}[X] \twoheadrightarrow \mathbb{F}_p[X] \twoheadrightarrow \mathbb{F}_p[X]/(X^2 + X + 1),$$
where the first map is the reduction of the coeficients modulo p and the second is the quotient map. The kernel of this map is $(p, X^2 + X + 1)$, so have
$$\mathbb{Z}[X]/(p, X^2 + X + 1) \cong \mathbb{F}_p[X]/(X^2 + X + 1).$$
On the other hand, we have another surjective morphism
$$\mathbb{Z}[X] \overset{\mathrm{ev}_j}{\twoheadrightarrow} \mathbb{Z}[j] \twoheadrightarrow \mathbb{Z}[j]/p\mathbb{Z}[j],$$
where the first map is given by the evaluation of a polynomial at j. The kernel of the evaluation is $(X^2 + X + 1)$. Indeed, it is clear that $(X^2 + X + 1) \subset \ker \mathrm{ev}_j$. On the other hand, if $P(j) = 0$, then $X^2 + X + 1 | P$ in $\mathbb{Q}[X]$ and by Gauss's Lemma $X^2 + X + 1 | P$ in $\mathbb{Z}[X]$. It follows that the kernel of the composition is $(p, X^2 + X + 1)$ which gives the desired isomorphism.

   d) By 1a and 1c, we have that p is not prime in $\mathbb{Z}[j]$ if and only if $(X^2 + X + 1)$ is not a maximal ideal of $\mathbb{F}_p[X]$, which is true iff $X^2 + X + 1$ has a root in $\mathbb{F}_p$. Since the discriminant of this polynomial is -3, this is true if and only if -3 is a square modulo p.

   e) Assume that $3 | p - 1 = |\mathbb{F}_p^\times|$. Then there exists an element $\alpha \in \mathbb{F}_p^\times$ of order 3. Thus $0 = \alpha^3 - 1 = (\alpha - 1)(\alpha^2 + \alpha + 1)$. Hence $X^2 + X + 1$ has a root so -3 is a square modulo p by 1d. If -3 is a square mod p, then the root of the polynomial $X^2 + X + 1$ has order 3 in the group $\mathbb{F}_p^\times$, so $3 || \mathbb{F}_p^\times| = p - 1$.

   f) Observe first that
$$\mathrm{N}\left(a + b\frac{-1 + \mathrm{i}\sqrt{3}}{2}\right) = a^2 - ab + b^2.$$

Now assume that $p \equiv 1 \bmod 3$, then p is not prime in $\mathbb{Z}[j]$, so $p = \pi_1\pi_2$ with π_i non units. It follows that $p^2 = \mathrm{N}(p) = \mathrm{N}(\pi_1)\,\mathrm{N}(\pi_2)$ which gives $\mathrm{N}(\pi_i) = p$. Conversely, if $p = \mathrm{N}(\pi)$ for some $\pi \in \mathbb{Z}[j]$, then p cannot be prime. Otherwise $p = \pi\overline{\pi}$ implies that $p|\pi$ and thus $\mathrm{N}(\pi) \geqslant p^2$.

2.

3.

4. The following codes provide solutions to the exercise. For part (d) of the exercise, the (correct) conjecture is that $\Omega_{c,T}(\alpha, \beta) \to |\beta - \alpha|$ as $T \to \infty$.

```
# import the time module to compare running times for the
# different algorithms
import time

# PRE:      odd prime p equivalent to 1 mod 4
# POST:     return value is the list of Gaussian integers (as
#           complex numbers) whose norm equals p
def FindReps(p):
    if (p in Primes()) and (p == mod(1,4)):
        # Used for timing the algorithm.
        # Set starting time here
        tic = time.perf_counter()
        # Define the field with p elements
        k = GF(p)
        # Find a square root of p-1 in k
        root = k(p-1).square_root()
        # if x is an element in k, then x.lift() is a representative
        # of x in ZZ
        m = root.lift()
        K.<i> = NumberField(x^2+1)
        OK = K.ring_of_integers()
        z = gcd(OK(p),OK(m+i))
        units = [1,-1,i,-i]
        reps = []
        for s in units:
            L = (s*z).complex_embeddings()
            reps.append(L[0])
            reps.append(L[1])
        toc = time.perf_counter()
        return reps
    else:
        print('Invalid input. ' +
                'Input must be a prime of residue 1 mod 4.')

# PRE:      List L of complex numbers, real number d != 0
# POST:     List L, entrywise divided by d
def DivideListOfComplex(L,d):
    for i in range(len(L)):
        L[i] = L[i] / d
    return L

# PRE:      Numbers c in (0,1) and T > 0
# POST:     A plot of the representations of admissible
#           primes between cT and T renormalized T^1/2
def DistributionAnnulus(c,T):
    L = []
    n = ceil(c*T)
    p = next_prime(n)
    while p <= T:
        p = next_prime(p)
```

```
        if p == mod(1,4):
            M = DivideListOfComplex(FindReps(p),sqrt(T))
            for i in range(len(M)):
                L.append(M[i])
    P = circle((0,0),1,rgbcolor = (0,0,0))
    P += circle((0,0),sqrt(c),rgbcolor = (1,0,0))
    P += point(L)
    P.show()

# PRE:      Numbers c, a<b in (0,1) and T > 0
# POST:     The share of the representations of admissible
#           primes between cT and T renormalized by T^1/2
#           which lie in the sector defined
#           by 2*pi*a to 2*pi*b
def Sampling(c,a,b,T):
    L = []
    n = ceil(c*T)
    p = next_prime(n)
    K = 0
    N = 0
    while p <= T:
        p = next_prime(p)
        if p == mod(1,4):
            M = DivideListOfComplex(FindReps(p),sqrt(T))
            for i in range(len(M)):
                N += 1
                phi = CC(M[i]).arg()
                if 2*pi*a <= phi and 2*pi*b >= phi:
                    K += 1
    return RR(K/N)
```

Listing 1. Example SageMath code for Ex. 5