健壮性：系统在不正常输入或不正常外部环境下仍能够表现正常的程度

正确性：永不给用户错误的结果

健壮性：尽可能保持软件运行而不是总是退出

正确性倾向于直接报错(error)，健壮性则倾向于容错(fault-tolerance)

对外的接口，倾向于健壮；对内的实现，倾向于正确

Steps for improving robustness and correctness

- **Step 0: To program code with robustness and correctness objectives using assertions, defensive programing, code review, formal validation, etc**
- **Step 1: To observe failure symptoms (Memory dump, stack traces, execution logs, testing)**
- **Step 2: To identify potential fault (bug localization, debug)**
- **Step 3: To fix errors (code revision)**

内部错误：程序员通常无能为力，一旦发生，想办法让程序优雅的结束

异常：你自己程序导致的问题，可以捕获、可以处理

Avoid putting executable code in assertions

- **Since assertions may be disabled, the correctness of your program should never depend on whether or not the assertion expressions are executed.**
- **In particular, asserted expressions should not have *side-effects*.**
  - For example, if you want to assert that an element removed from a list was actually found in the list, don't write it like this:
- **If assertions are disabled, the entire expression is skipped, and x is never removed from the list. Write it like this instead:**

```
// don't do this:
assert list.remove(x);
```

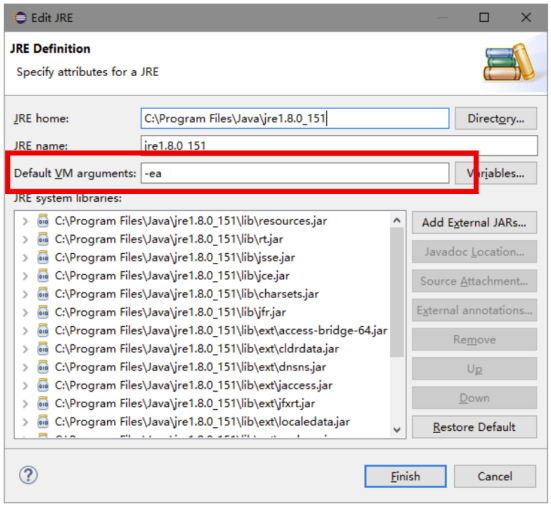
```
// do this:
boolean found = list.remove(x);
assert found;
```

不要再assert语句中进行判断以外的操作

程序之外的事，不受你控制，不要乱断言

Enable & Disable assertions in Java

- **Enable assertions**
  - Running the program with the `-enableassertions` or `-ea` option:
    - `java -enableassertions MyApp`
  - The option -ea... turns on assertions in all classes of the default package.
    - `java -ea:MyClass MyApp`
- **Disable assertions**
  - Running the program with the `-disableassertions` or `-da` option:
    - `java -ea:... -da:MyClass MyApp`
- **By default, assertions are disabled.**
- **Enable assertions in Eclipse:**
  - In preferences, go to Java → Installed JREs . Click "Java SE 8", click "Edit…", and in the "Default VM arguments" box enter: `-ea`



Assertion vs. Exception?

- **Use error handling code (exception) for conditions you expect to occur 使用异常来处理你"预料到可以发生"的不正常情况**
  - Error handling code checks for off-nominal circumstances that might not occur very often, but that have been anticipated by the programmer who wrote the code and that need to be handled by the production code.
- **Use assertions for conditions that should never occur 使用断言处理"绝不应该发生"的情况**
  - Assertions check for bugs in the code.

断言可用于private的方法或者用于检查post-condition